802.11g Wireless Outdoor Access Point/Ethernet Bridge

Revision 2.6

User Guide

FCC Notice

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed

and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate the equipment.

The Wireless Technology

Standard

The Wireless Access Point utilizes the 802.11b and the 802.11g standards. The IEEE 802.11g standard is an extension of the 802.11b standard. It increases the data rate up to 54 Mbps (108Mbps in Super G mode) within the 2.4GHz band, utilizing OFDM technology. This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format you're your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing OFDM (Orthogonal Frequency Division Multiplexing) technology. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of cross talk (interference) in signal transmissions. The AP will automatically sense the best possible connection speed to ensure the greatest speed and range possible. 802.11g offers the most advanced network security features available today, including: WPA, TKIP, AES and Pre-Shared Key mode.

Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network. The wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router. An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, providing that they both share the same channel and SSID. Before enabling you consider roaming, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

Network Layout

The AP Access Point has been designed for use with 802.11g and 802.11b products. With 802.11g products communicating with the 802.11b standard, products using these standards can communicate with each other. The Access point is compatible with 802.11g and 802.11b adapters, such at the PC Cards for your laptop computers, PCI Card for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity. These wireless products can also communicate with a 802.11g or 802.11b wireless Print Server. When you wish to connect your wired network with your wireless network, the Access Point’s network port can be used to connect to any of switches or routers.

Installation Considerations

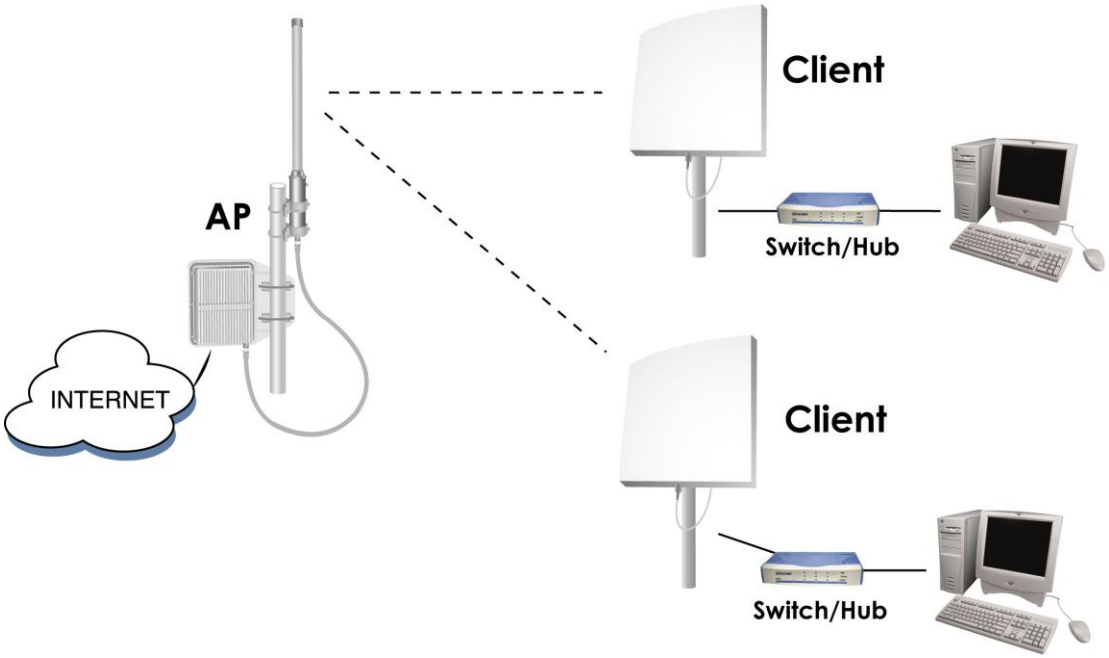
The AP lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
- Keep the number of walls and ceilings between the AP and other network devices to a minimum - each wall or ceiling can reduce your AP’s range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick(.5 meters), at a 45-degree angle appears to be almost 3 feet (1

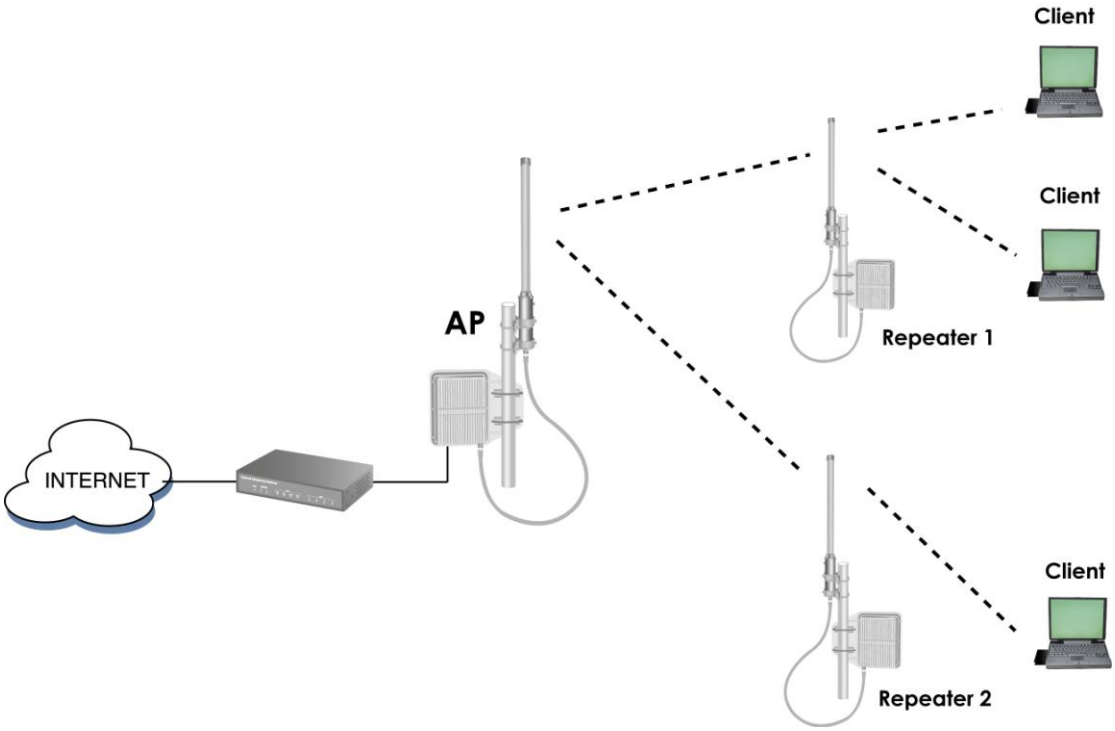
meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

- Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

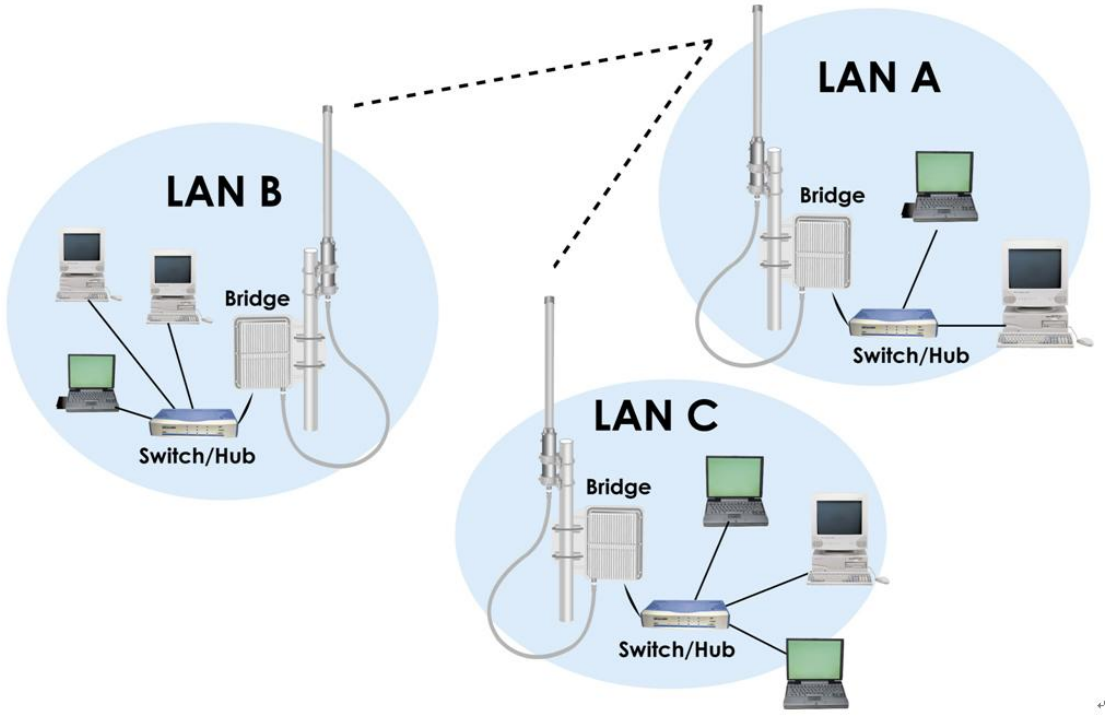
Network Topology – AP Mode and Client Mode



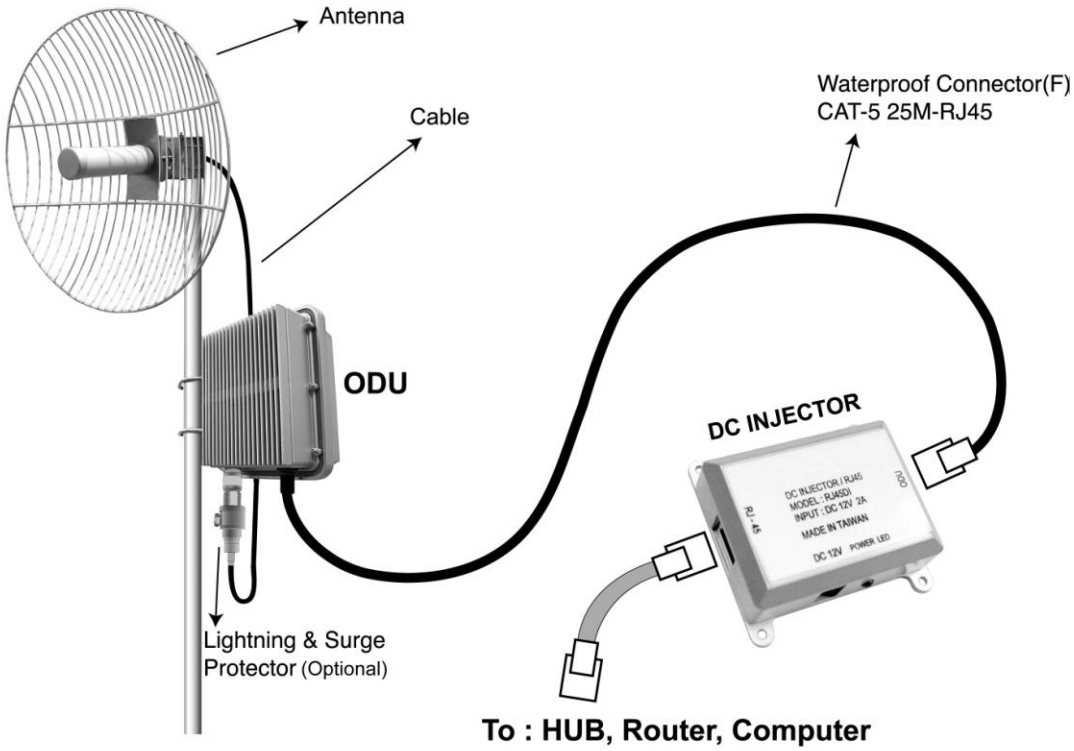
Network Topology – Repeater Mode



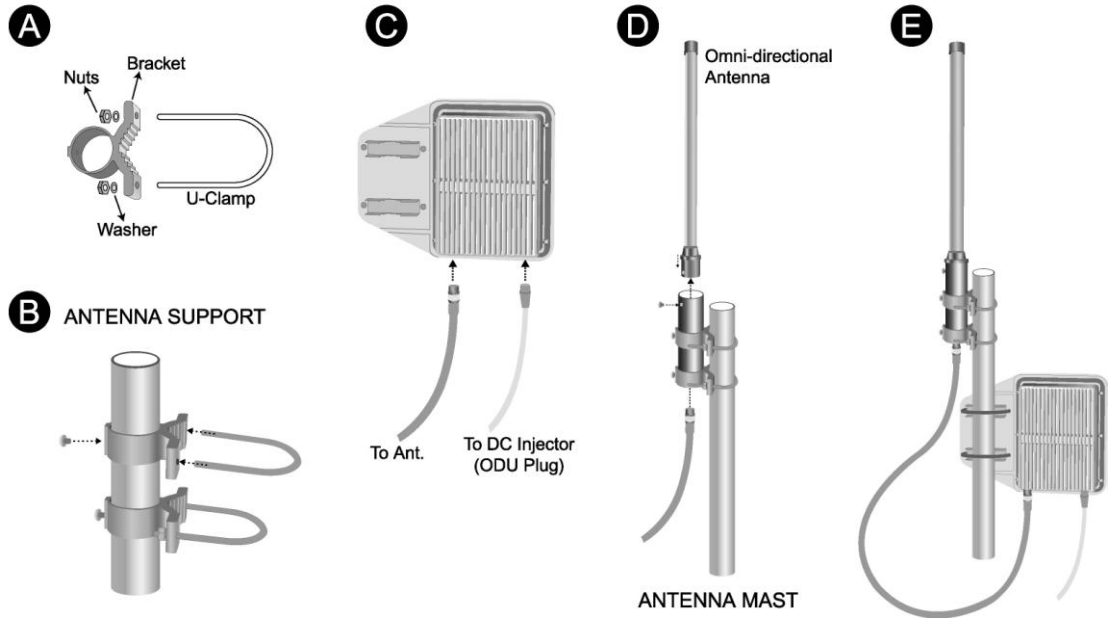
Network Topology – Wireless Bridge (WDS) Point to Multi-Point Mode



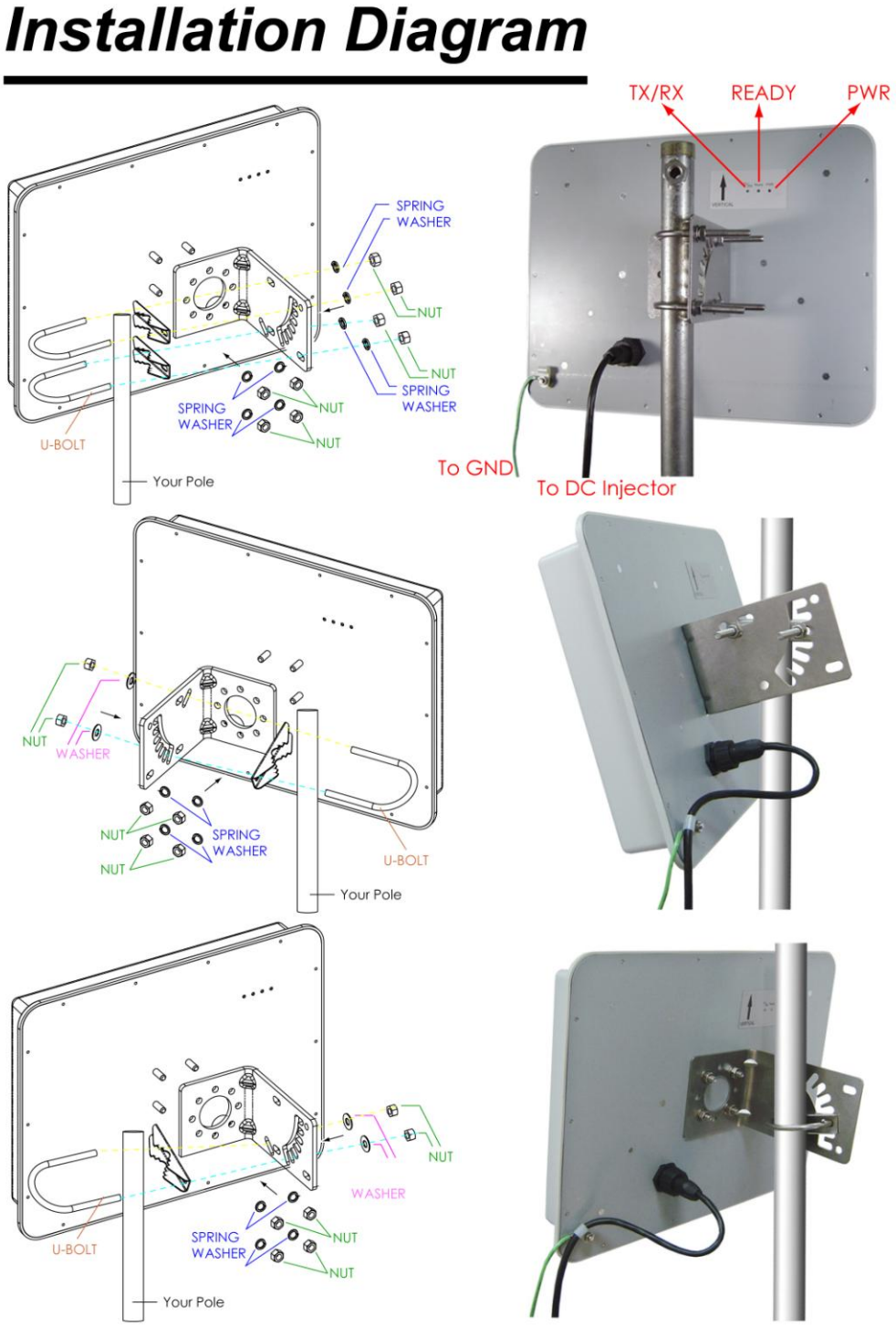
Installation Diagram



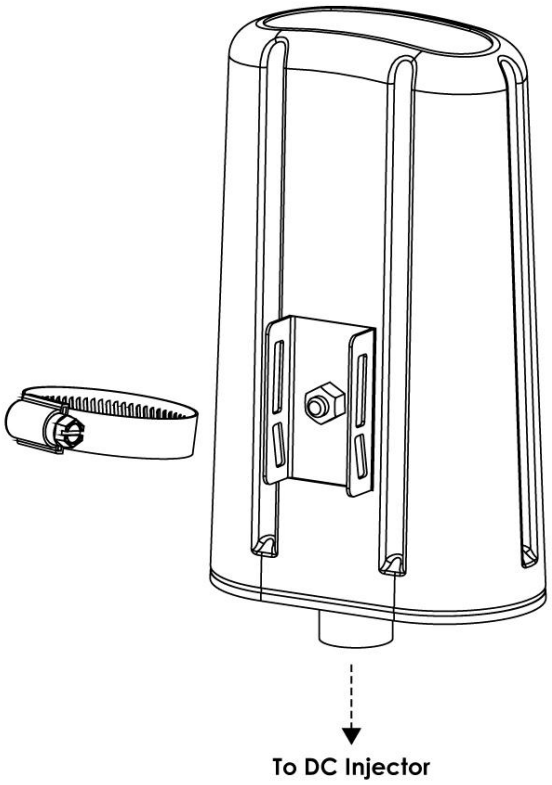
Omni-Directional Antenna Installation Diagram



CPE Installation Diagram



ASU Installation Diagram

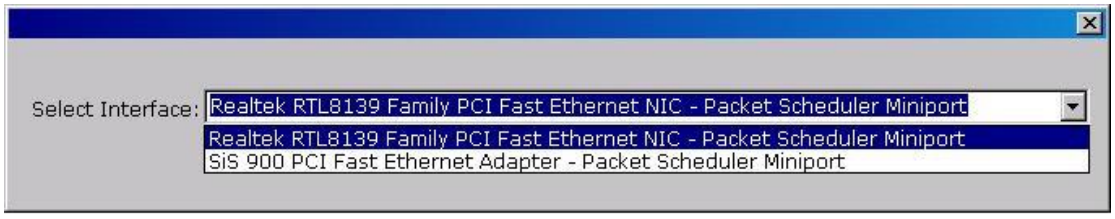


Attention:

- The cable distance between the Router and PC/hub/Switch should not exceed 100 meters.
- Make sure the wiring is correct. In 10Mbps operation, Category 3/4/5 cable can be used for connection. To reliably operate your network at 100Mbps, you must use Category 5 cable, or better Data Grade.

AP Configuration Using Locator

While entering the Locator utility, the Locator will automatically search the AP available on the same network. Locator will show the Device Name, Device Type, IP Address, Ethernet MAC Address and Firmware Version in first page. Before start using Locator, make sure you disable personal firewall installed in you PC. (Ex. Windows XP personal firewall)


Select Interface:
Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
SiS 900 PCI Fast Ethernet Adapter - Packet Scheduler Miniport

If you have 2 Fast Ethernet Adapter or more, you can choose enable one Fast Ethernet Adapter for enter with Locator utility.

AP Configuration Using Web User Interface

Before Setup...

❖ Verify the IP address setting

You need to configure your PC's network settings to obtain an IP address. Computer use IP addresses to communicate with each other across a network, such as the Internet.

1. From the taskbar, click the **Start** button, select **Settings** > **Control Panel**. From there, double-click **the Network connections** icon.
2. Right click the **Local Area Connection** icon **Properties**; select the **TCP/IP** line for the applicable Ethernet adapter. Then, click the **Properties** button.
3. Click the **IP Address** tab page, select **USE the following IP address**, type **192.168.254.254** (but, **192.168.x.x** for the device use) in the **IP Address** field and **255.255.0.0** in the **Subnet Mask** field, then click **OK** button.

Start Setup by Browser...

1. After getting the correct connection, start the web browser (make sure you disable the proxy) and type **192.168.x.x (x is outdoor unit ip Address)** in the **Address** field. Press **Enter**.

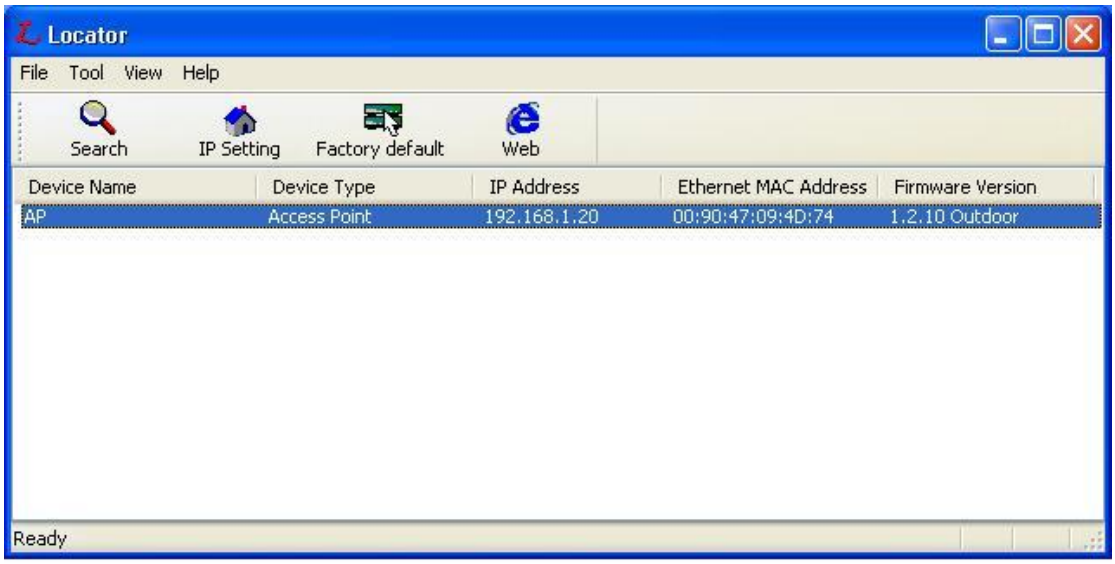
2. Enter the factory default ***User name*** and ***Password*** fields:

User Name: **Admin**
Password: **(leave blank)**
then click **OK** button.

3. You will enter the Utility homepage.

Start Setup by Locator...

1. You just need to click on the "**Web**" icon in Locator main page. The Locator will launch a default browser for you and lead you into web UI directly

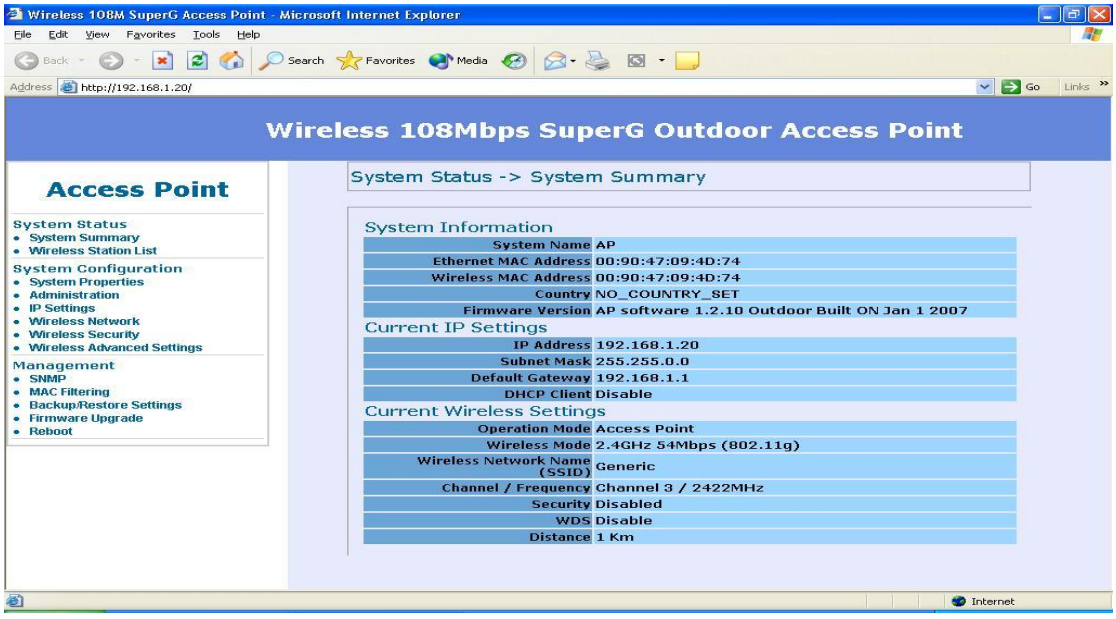


Wireless Configuration - AP Mode

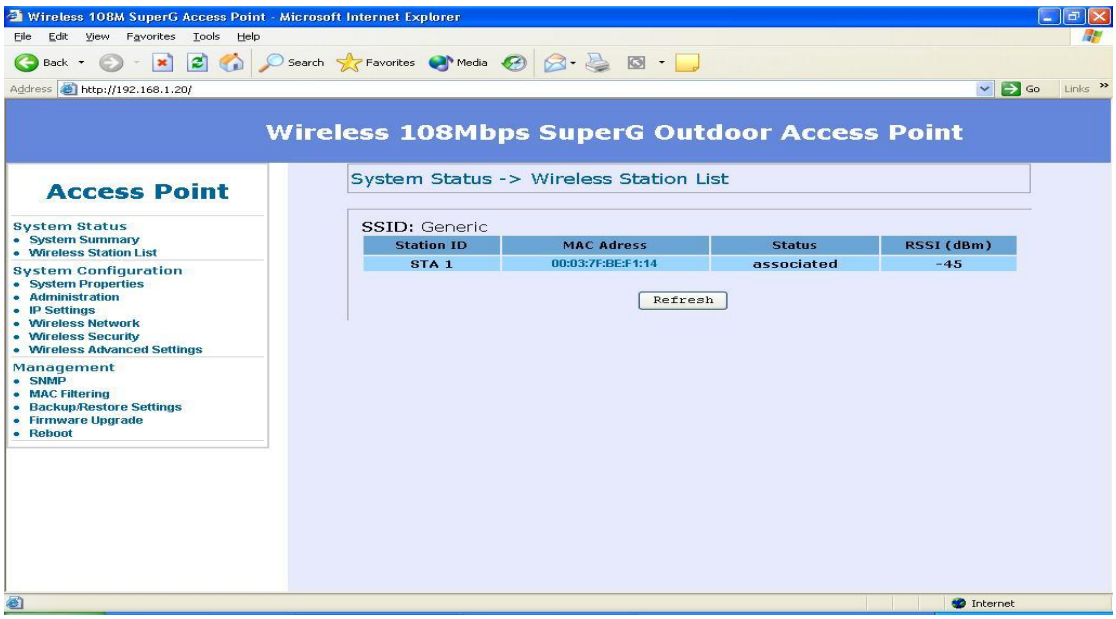
System Status –

The first page appears in main page will show "**System Status** -> **System Summary**" automatically, you can find detail system configuration in this page including

- **System Information –** This will display system name and both Ethernet MAC address and Wireless MAC address. Current country setting and firmware version will also be available here.
- **Current IP Settings –** This section show current IP address setting including IP address, Subnet Mask, Default Gateway and DHCP status.
- **Current Wireless Settings** – This area show current wireless setting including operation mode, wireless mode, SSID, Channel/Frequency, security setting, WDS mode and Distance..



The first page appears in main page will show “**System Status** -> **Wireless Station List**” automatically, this page can help user identify current devices who already associated to the AP. You can also click on the MAC address column then the system will show the detail technical information for each wireless station.



Clicking MAC address hyperlink of desired remote devices, system will show a Statistics page for you to monitor the information of the remote link.

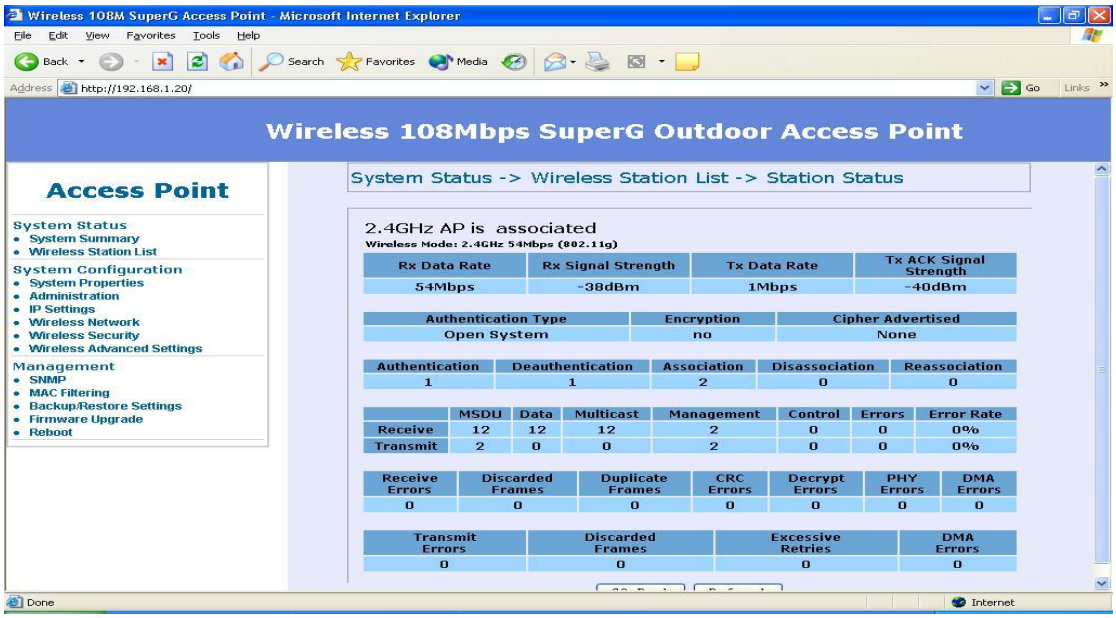
Values on this page are automatically refreshed every **minute**. You may manually press the refresh button of browser to get the updated data more frequent. As RF signal strength is more critical for outdoor deployment purpose, **RSSI** bar is refreshed every **2** seconds.

Note: Due to frequent refresh of Statistics page, it is strongly recommended that you close this page when performing network performance tests.

Field	Description
RSSI	Displays the strength of the received signal in dBm (the remote devices received signal strength). Refresh every 2 seconds.
RSSI of ACK	Displays the strength of the ACK signal from far end in dBm (the local devices received signal strength). Refresh every 2 seconds.

MSDU	Maximum service data unit. Displays the number of packets sent and received by the remote devices.
Data / Management / Control	Packets can be data, management or control. Displays the number of packets sent and received for each.
Multicast	Displays the number of multicast frames.
Data Rate	Displays the receive and transmit data rate in Mbps.
Receive Errors	Displays the number of receive errors.
Discarded Frames	Displays the number of receive discarded frames.
Duplicate Frames	Displays the number of receive duplicate frames.
CRC Errors	Displays the number of receive CRC errors.
Decrypt Errors	Displays the number of receive description errors.
PHY Errors	Displays the number of receive PHY errors.
DMA Errors	Displays the number of receive DMA errors.
Transmit Errors	Displays the number of transmit errors.
Discarded Frames	Displays the number of transmit discarded frames.
Excessive Retries	Displays the number of transmit excessive retries.
DMA Errors	Displays the number of transmit DMA errors.

The page below describes the detail connection information with each station. You can get all information needed right here.



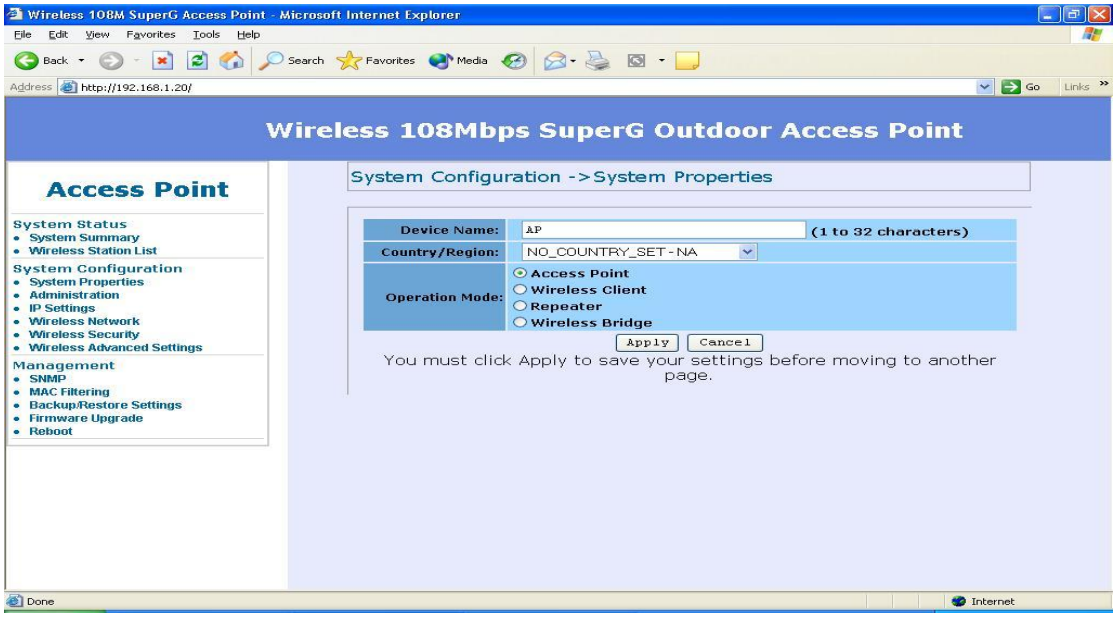
System Configuration –

Now you can start to configure the system. In **System Properties** page, you can config

- **Device Name –** You may assign any name to the Access Point. Memorable, Unique names are helpful especially if you are employing multiple access points on the same network. The device name needs to be less than 32 characters. After verify the name you input and click "**Apply"** to save the setting.
- **Country/Region** – Here you can set the AP to follow different country and region regulation. The AP can support

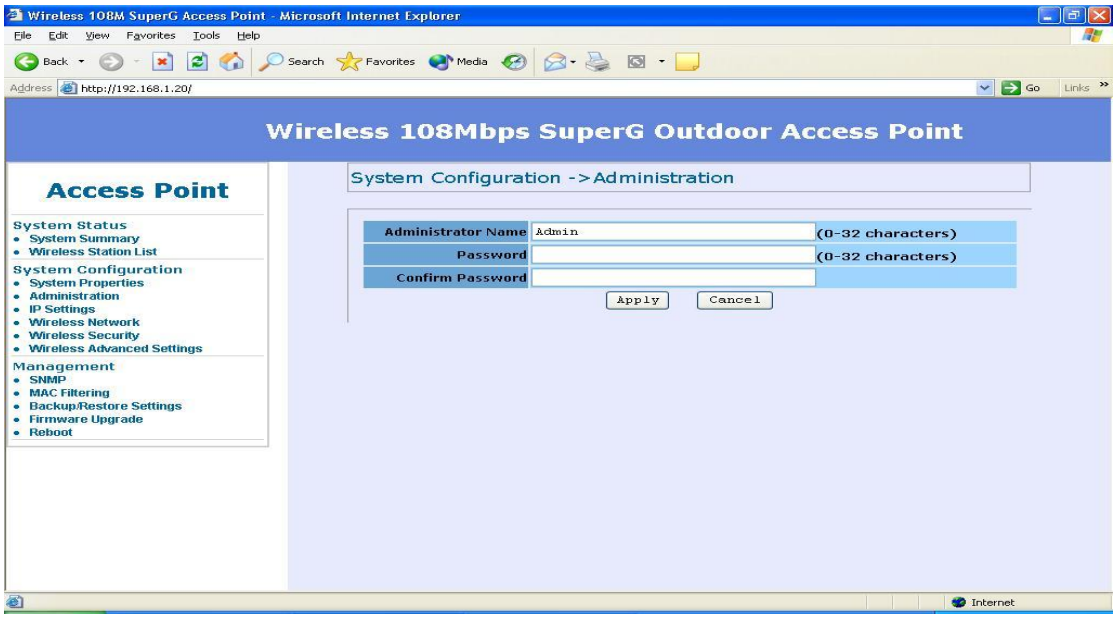
- **Operation Mode** - The default operation mode is Access Point, this connects your wireless PCs and devices to a wired network. In most cases, no change is necessary. You can switch operation mode to Wireless Client or Repeater or Bridge mode depends on your application. Wireless Client mode can allow AP act as a client within its range. Your Ethernet devices behind the AP can connect to remote AP. Repeater is able to talk with one remote access point within its range and retransmit its signal. Choose repeater mode if you want to extend the range of your original AP. Wireless Bridge (WDS) can allow Bridge point to point or point to multi-point network architecture, In order to establish the wireless link between bridge radios, the MAC address of remotes bridge(s) need to be

registered in the address table. Type the MAC address with format xx:xx:xx:xx:xx:xx (x is the hexadecimal digit) and use “Add” and “Delete” button to edit the address table. A Master Bridge Radio may accommodate *up to* ***8*** remote MAC addresses.



Administration –

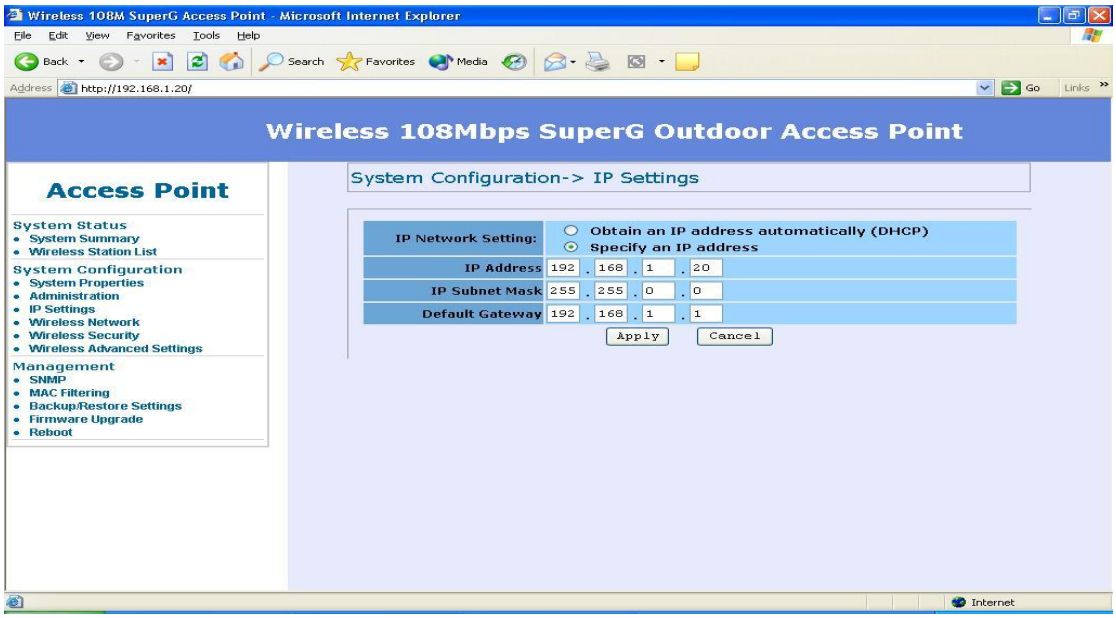
In the administration page, you can modify “**Administrator Name**” and “**Password**”. Changing the sign-on user name and password is as easy as typing the string you wish in the column. Then, type the password into second column to confirm. Click **“Apply”** to finish the procedure. Be sure you noted the modification before apply all changes.



IP Settings –

IP Setting page can configure system IP address. Default IP address is 192.168.x.x and Subnet Mask is 255.255.0.0. You can manually input IP address setting or get an IP from a DHCP server.

- **IP Network Setting –** Here you can choose to get IP from a DHCP server or specify IP address manually. Choose to obtain an IP address from DHCP server if your environment or ISP provide DHCP server. Otherwise, you can manually setup IP address.
- **IP Address –** The IP address need to be unique to your network. We would like to recommend you stay with default IP address 192.168.x.x. This is private address and should work well with your original environment.
- **IP Subnet Mask –** The Subnet Mask must be the same as that set on your Ethernet network.
- **Default Gateway –** If you have assigned a static IP address to the Access Point, then enter the IP address of your network's Gateway, such as a router, in the Gateway field. If your network does not have a Gateway, then leave this field blank.



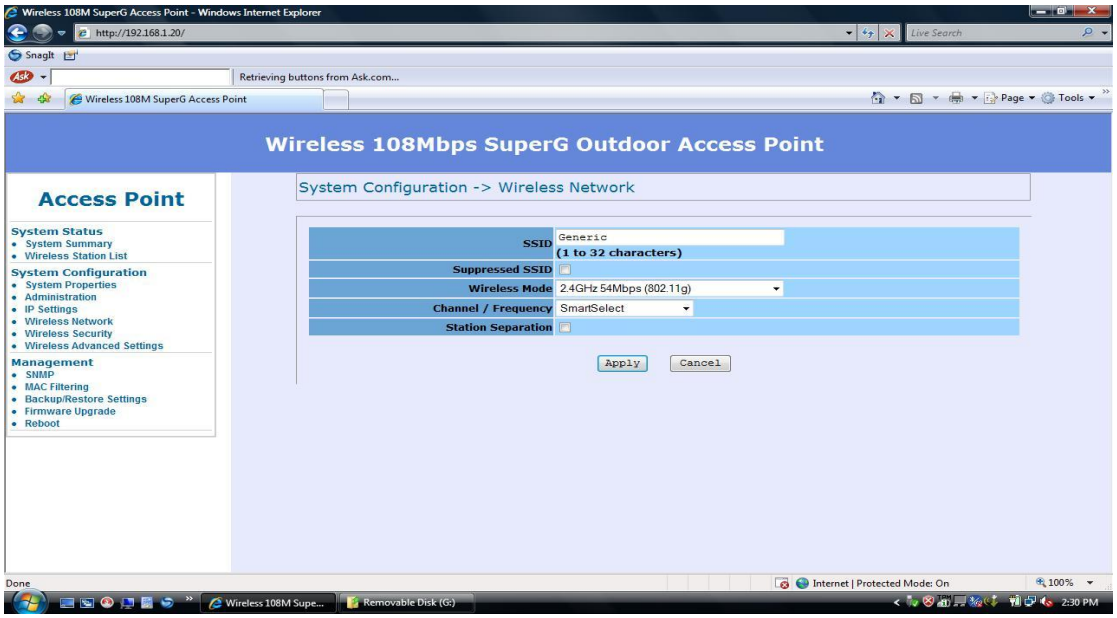
Wireless Network -

At Wireless Network page can set "**SSID**" / "**Wireless Mode**" and "**Channel**". AP supports not only standard 11b/g but also 108M SuperG. (Note: 108 M SuperG only works with Atheros® based 11b/g solution)

- **Wireless Network Name (SSID) -** The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. For added security, you should change the SSID from the default name **Generic**, to a unique name.
- **Suppressed SSID –** This option can hide the SSID not available from site survey tool. Enable this function only if you do not want the Access Point to be found by others.
- **Wireless Mode –** Default setting is **"2.4GHz 54Mbps (802.11g)"**. This will support all 802.11b/g clients connect to the AP. You can choose **"2.4GHz 11Mbps (802.11b)"** in wireless mode column if your environment only have 802.11b clients. The final selection **"2.4GHz 108Mbps (802.11 SuperG)"** supports high speed 108Mbps SuperG function. In order to support SuperG 108M transmission, all wireless clients will need to be Atheros® solution.
- **Channel / Frequency –** Select the appropriate channel from the list provided to correspond with your network settings. All points in your

wireless network must use the same channel in order to function correctly. The default setting is **"Smart Select"** means the system will pick best channel for you automatically. Stay with default setting if you do not have special request on channel selection.

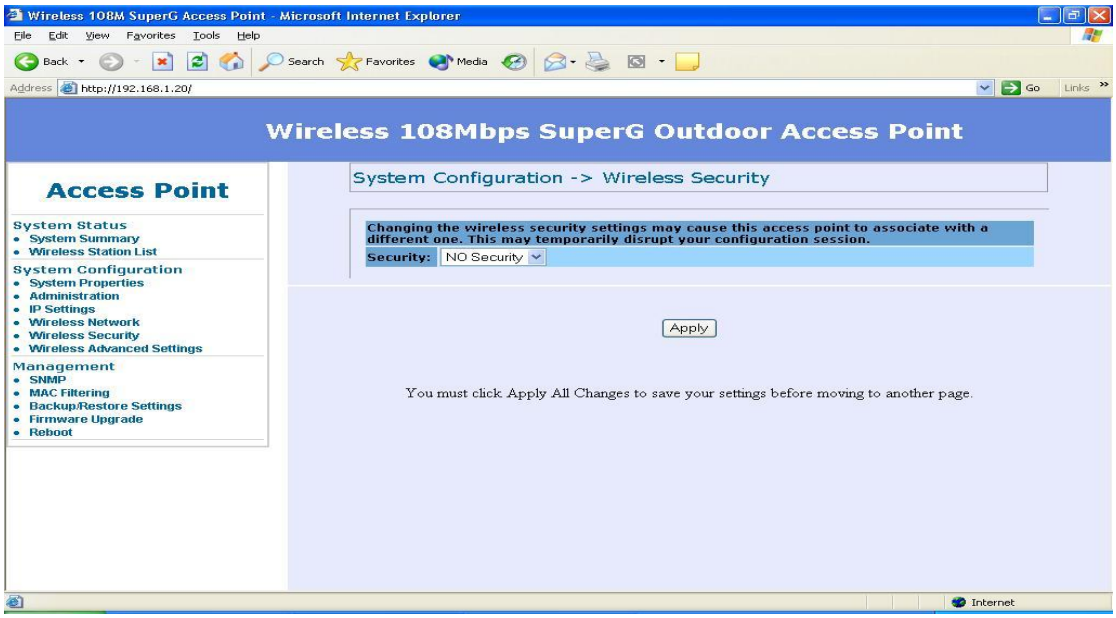
- **Stations Separation –** Default setting is **"Disable"**. This option can disallow the client devices connected to this AP could not access each other.



Wireless Security -

The wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Access Point: WEP, WPA-PSK and WPA. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.)

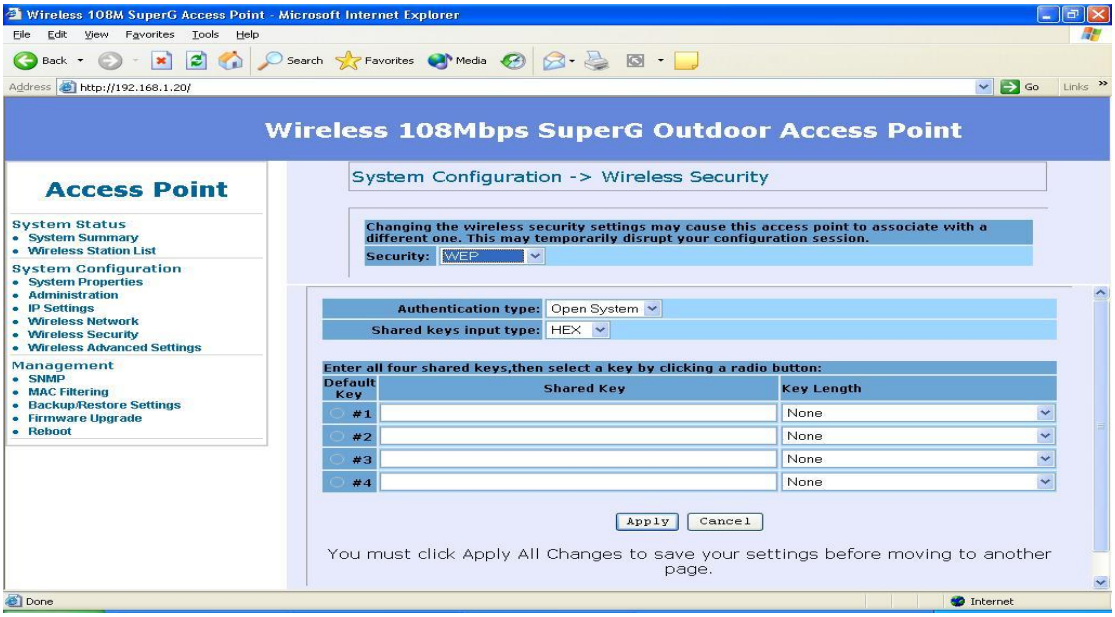
In Wireless Security page, you can configure the AP to work with **No Security**, **WEP**, **WPA-PSK** and **WPA** security mode. Once you setup the AP to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is **"No Security"**.



WEP is a basic encryption method, which is not as secure as WPA. To use WEP, you will need to select a default transmit key and a level of WEP encryption,

- **Authentication type –** Select **“Open System”** to communicate the key across the network. Select “Share Key” to limit communication to only those devices that share the same WEP settings.
- **Shared keys input type –** Select HEX or ASCII depends on your preference
- **Key table –** You can input 4 different WEP encryption keys into the table and by choosing the radio button to decide which one is valid now. The AP supports 64, 128 and 152bit key length. The longer key we choose usually means the encryption is stronger.

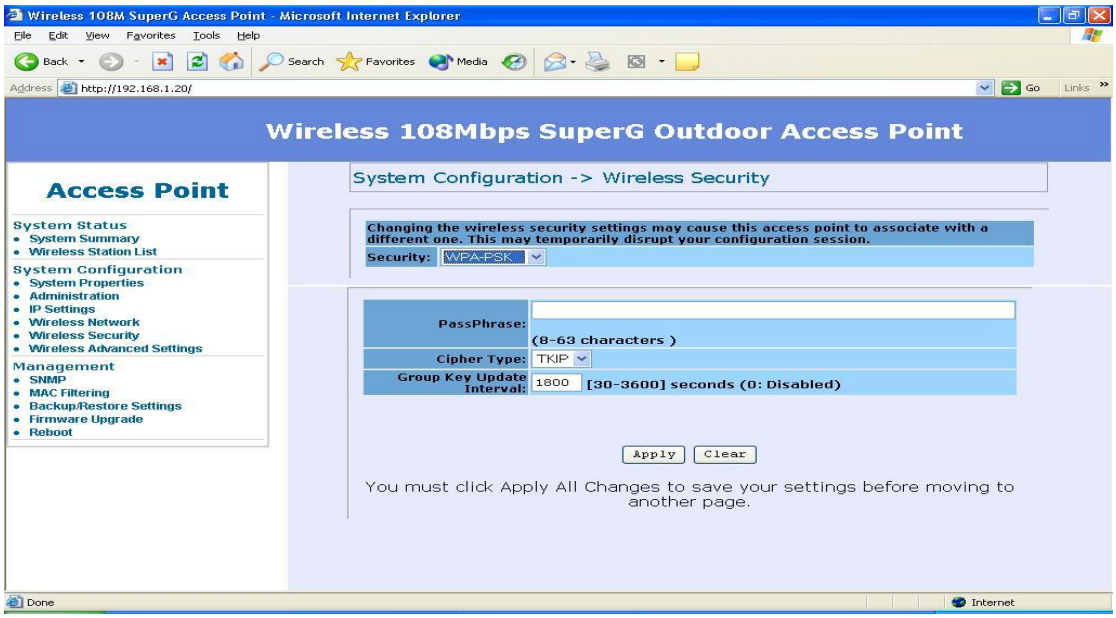
After all changes are made, be sure to click on **“Apply”** to make sure all changes are saved into system.



WPA-PSK stands for Wi-Fi Protected Access – Pre-Shared Key. WPA-PSK is design for home users who do not have RADIUS server in their network environment. WPA can provide better security level than WEP without difficult setting procedure.

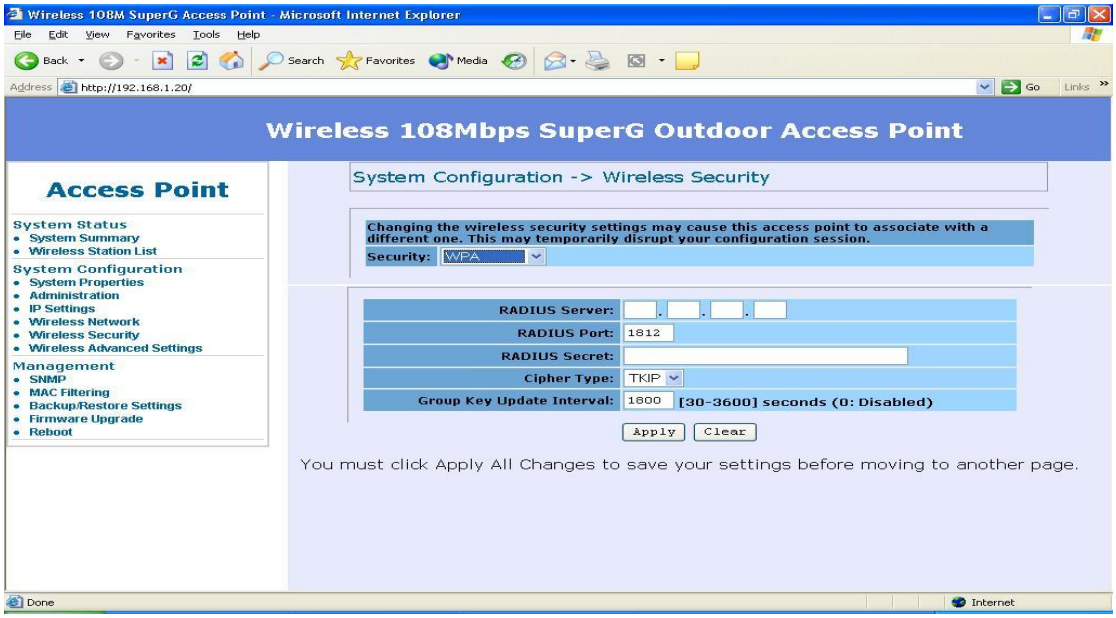
- **PassPhrase -** Enter a WPA Shared Key of 8-63 characters. The Shared Key should be also applying the clients work in the same wireless network.
- **Cipher Type -** WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**.
- **Group Key Renewal period -** Enter a number of seconds which instructs the Access point how often it should change the encryption keys. Usually the security level will be higher if you set the period shorter to change encryption keys more often. Default value is 1800 seconds, set 0 in Group Key Renewal period to disable key renewal.

Remember to click on **"Apply"** to make sure all changes are made before leaving this page.



WPA option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Access Point.)

- **RADIUS Server –** Here enter the IP address of your RADIUS server.
- **RADIUS Port –** Port number for RADIUS service, default value is 1812
- **RADIUS Secret –** RADIUS secret is the key shared between Access Point and RADIUS server.
- **Cipher Type –** WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**.
- **Group Key Update Interval –** This column indicate how often should the Access Point change the encryption key.



Wireless Advance Settings -

The page below can help users to configure advanced wireless setting. Before making any changes at this page, please check your wireless settings on other system as well, as these changes will alter the effectiveness of the Access Point. In most cases, these settings do not need to be changed.

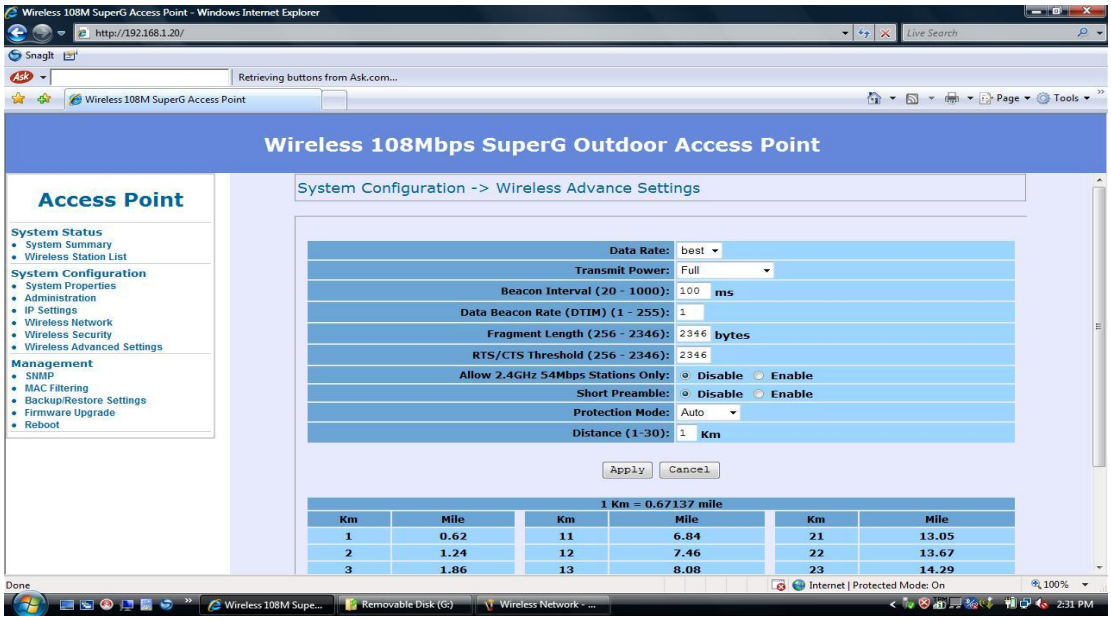
- **Data Rate –** In data rate column you can select all bit rate supported in current operation mode. Default value is "**best**" means the system will automatically adjust the connection speed dynamically according to your current link status.
- **Transmit Power –** You can reduce RF output power by selecting Half (-3dB) / Quarter (-6dB) / Eighth (-9dB) / Minimum. To change transmit power may decrease your wireless signal coverage.
- **Beacon Interval (20-1000) –** This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination address, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).
- **Data Beacon Rate (DTIM) (1-16384) –** This value indicated how often the Access Point sends out a Delivery Traffic Indication Message. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.
- **Fragment Length (256-2346) –** This specifies the maximum size a data packet will be before splitting and creating a new packet and should remain at its default setting of 2,346. A smaller setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.
- **RTS/CTS Threshold (256-2346) –** This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. Should you encounter inconsistent data flow, only minor modifications are recommended.

- **Allow 2.4GHz 54Mbps Stations Only –** Default setting is **"Disable"**. Select **"Enable"** all of your wireless clients are 802.11g mode, if you select "Disable" using both 802.11b and 802.11g wireless clients.
- **Short Preamble –** Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try to enable short preamble.

- **Protection Mode –** Protection Mode should remain default value (Auto) unless you are having severe problems with your 11g Wireless LAN products not being able to transmit to the Access Point in an environment with heavy 802.11b traffic. To enable this function boosts the Access Point's ability to catch all 11g Wireless transmissions but will severely decrease performance.

- **Distance (1-30) –** Setup "**Distance**" according to the longest link distance between the point to point or point to multi-point in the network. The input needs to be greater than or equal to the real distance. The range can be from *1KM to 30KM* for ***normal mode*** and *1KM to 15 KM* in ***Super mode***.

Remember to click on **"Apply"** to make sure all changes are made before leaving this page.

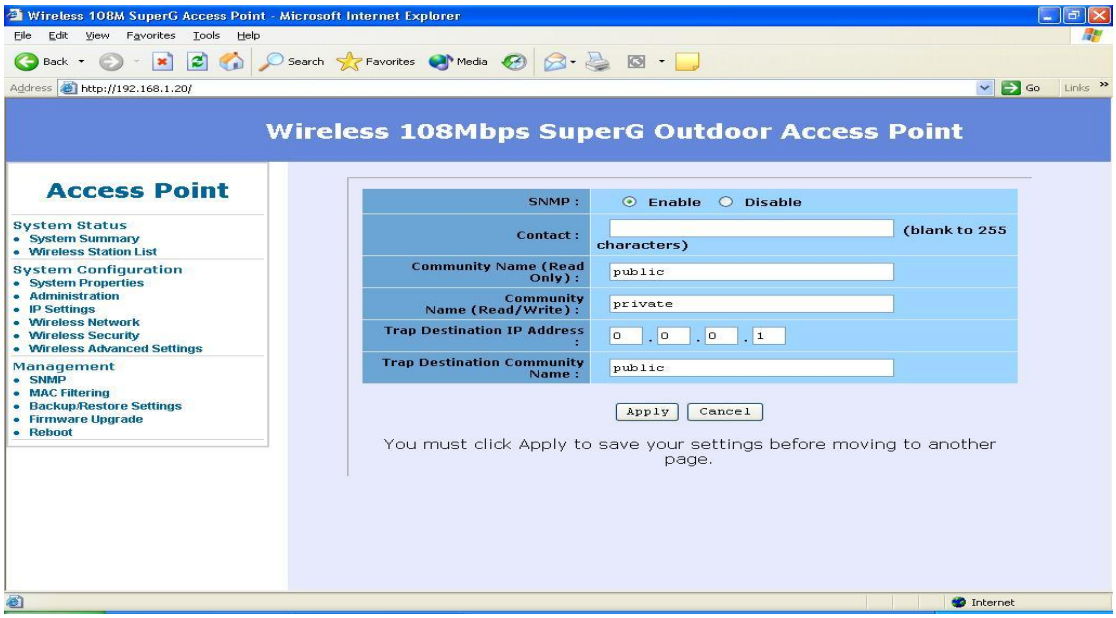


Changing SNMP Settings

Under System Configuration, click **SNMP** to display and change settings for the Simple Network Management Protocol.

To communicate with the access point, the **SNMP** agent must first be enabled and the Network Management Station must submit a valid community string for authentication. Select **SNMP** Enable and enter data into the fields as described below. When you are finished, click **“Apply”**

Setting	Description
SNMP	Enables or disables SNMP.
Contact	Sets the location string that describes the system location. Maximum length is 255 characters.
Community Name (Read Only)	Specifies a community string with read-only access. Authorized management stations are able to retrieve MIB objects. Maximum length is 32 characters.
Community Name (Read Write)	Specifies a community string with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. Maximum length is 32 characters.
Trap Destination IP Address	Enter the IP address of the trap manager that will receive these messages.
Trap Destination Community Name	Enter the community name of the trap manager that will receive these messages.



MAC Filtering

As an additional layer of security, MAC Filtering allows you to block network access of specified stations through the access point.

Enable MAC Filtering

You can click the Checkbox **MAC Filtering** to Enable MAC Filtering.

MAC Filtering Rule

- Select **Allow only station in list** to filter any MAC address that **NOT** listed in the **MAC Filtering Table**
- Select **Allow any station unless in list** to filter any MAC address that listed in the **MAC Filtering Table**

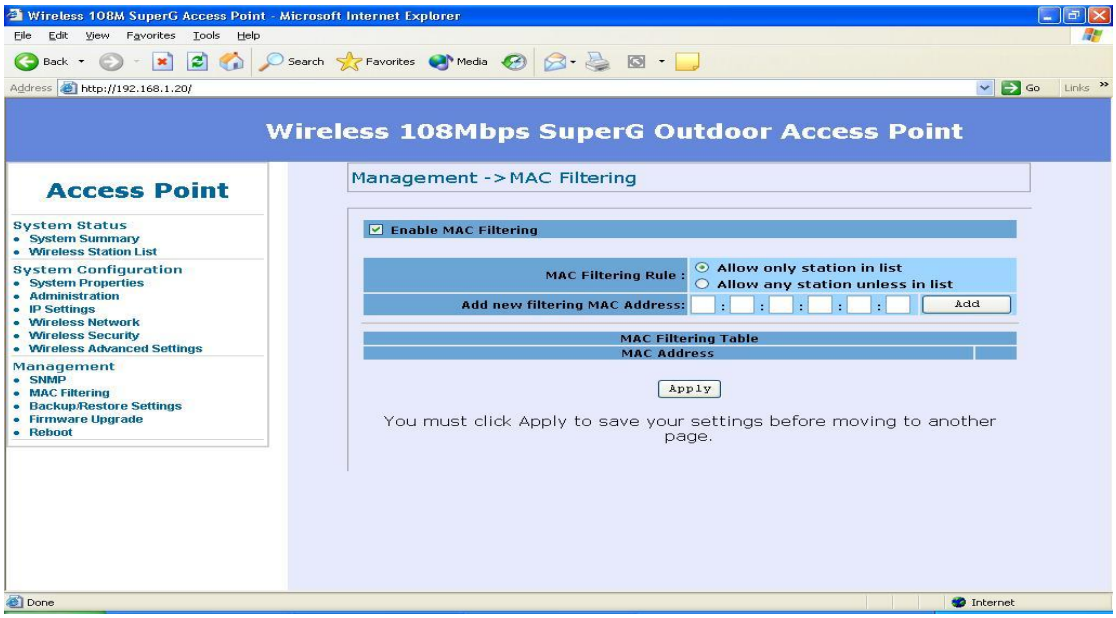
Add MAC Address

You can input MAC address and click Add to **add** MAC address into the **MAC Filtering Table.**

MAC Filtering Table

This lists any wireless stations you have entered. If you have not entered any wireless stations this list will be empty.

To delete an existing entry, select it and then click the **Delete** button.

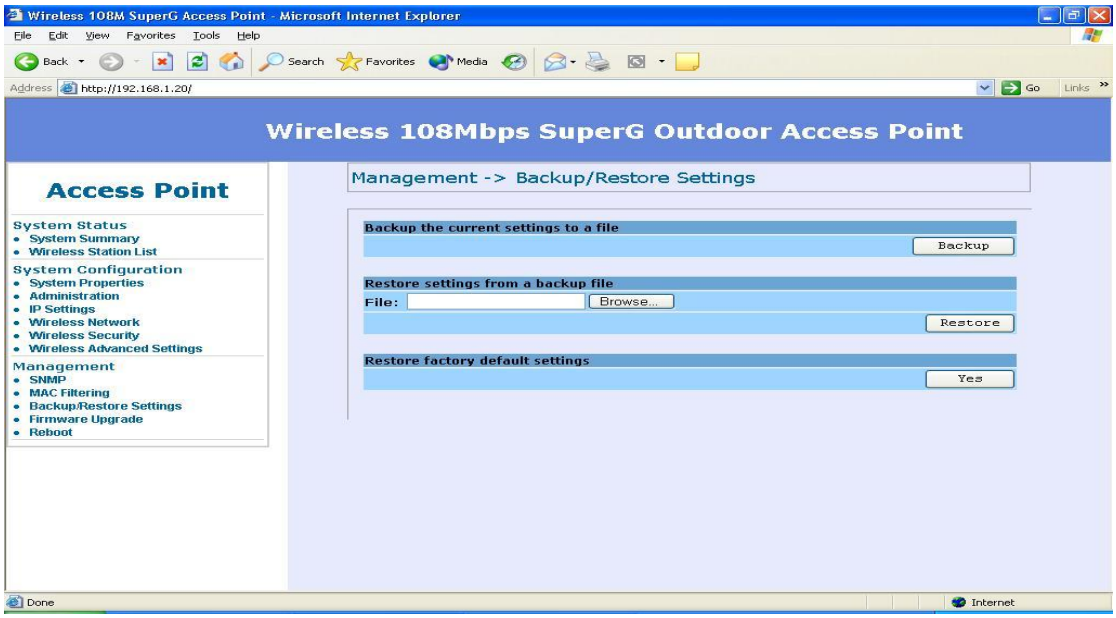


Backup/Restore Setting / Firmware Upgrade and Reboot -

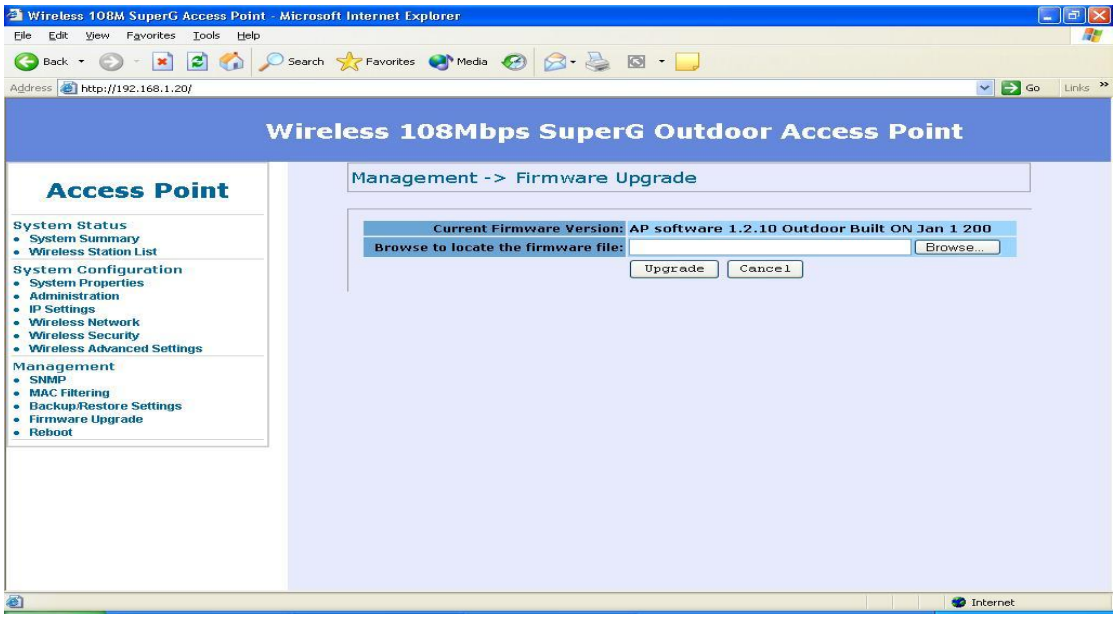
In Management section, you can **Backup/Restore Setting**, **Firmware Upgrade** and **Reboot** the system in following pages.

- **Backup the current settings to a file –** Click on the “Backup” button, system will prompt you where to save the backup file. You can choose the directory to save your configuration file.
- **Restore settings from a backup file –** Here you can restore the configuration file from where you previous saved.
- **Restore factory default setting –** Be very carefully before restore system back to default since you will lose all current settings immediately. If you act the function, the ip address will restore the establishing value situation.

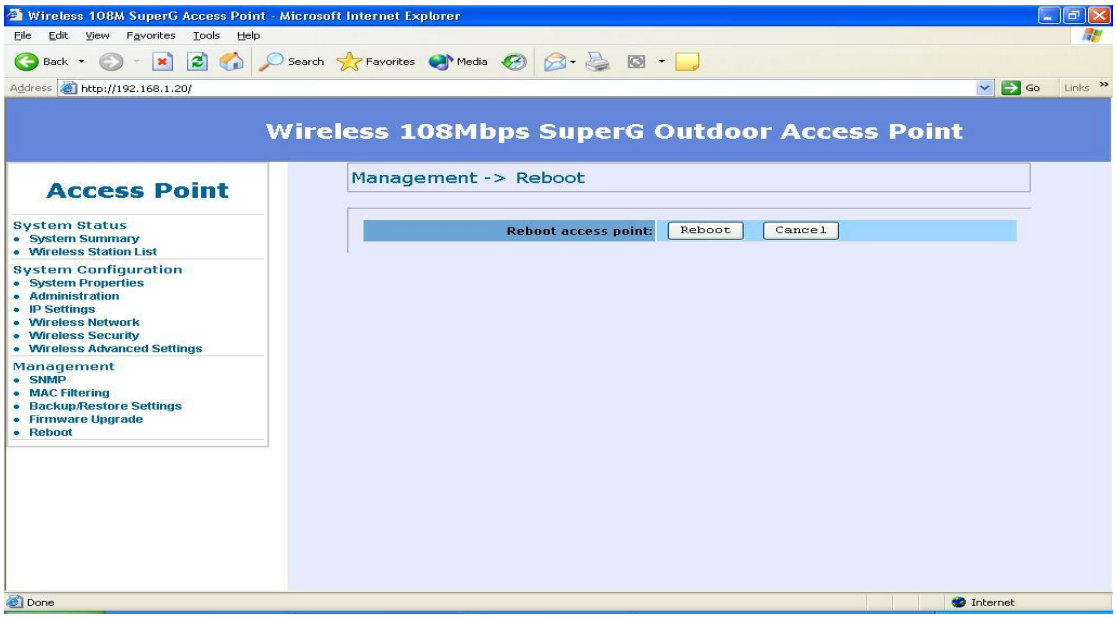
  192.168.1.20 in the **IP Address** field and **255.255.255.0** in the **Subnet Mask** field,



Firmware Upgrade – Enter the location of the firmware upgrade file in the file path field, or click the **"Browse"** button to find the firmware upgrade file. Then click on the **"Upgrade"** button, and follow the on-screen instructions. The whole firmware upgrade process will take around 60 seconds. Before upgrade, make sure you are using correct version. Please check with your technical support service if new firmware available.



Reboot – Click on **“Reboot”** button to restart Access Point.

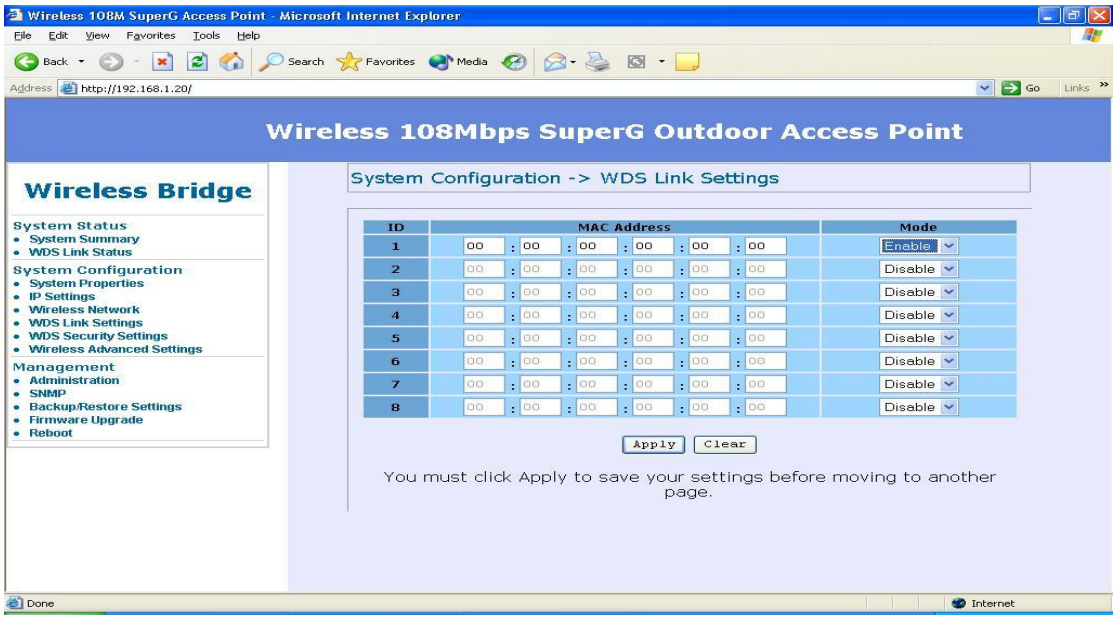


Wireless Configuration – Wireless Bridge (WDS) Mode (Point to Point & Point to Multi-Point)

Wireless Bridge is WDS (Wireless Distribution System) operation as defined by the IEEE802.11 standard has been made available. In IEEE 802.11 terminology a "Distribution System" is system that Interconnects, so-called, Basic Service Sets (BSS). A BSS is best compared to a "Cell", driven by a single Access Point (one of those circles in the diagram below). So a "Distribution System" connects cells in order to build a premise wide network which allows users of mobile equipment to roam and stay connected to the available network resources.

Wireless Bridge (WDS) is used for wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement. (Be sure you understand the purpose of WDS mode before proceed configuration.)

The Wireless Bridge (WDS) mode is coexisting with Wireless Bridge (WDS) mode in this AP, therefore, you can support regular wireless stations or WDS link. In the **“WDS Link Settings”**, check box and switch the **“Mode”** to **“Enable”**. Then you are able to fill in MAC Address of each WDS link Settings.



Considerations before installation –

- **Loop Prevention –** Be careful to plan you WDS connections, prevent your wireless network topology to have loop. Once loop shows up, you network traffic will become unstable.
- **Performance –** The system can support up to 8 WDS links. But all links and wireless stations that operate at the same time will all share single radio bandwidth. (Ex. 11g have 54Mbps bandwidth)
- **Latency –** In the chain topology configuration, if the chain becomes very long, end-to-end latency issue may come in play. We suggest the WDS link topology planning should not exceed 2 hops in chain configuration.

Wireless Bridge (WDS) Security Settings–

Wireless Bridge (WDS) now only supports limit wireless security protocol and will have full dependency with Access Point mode security settings. Here lists 4 different Wireless Bridge (WDS) security settings below:

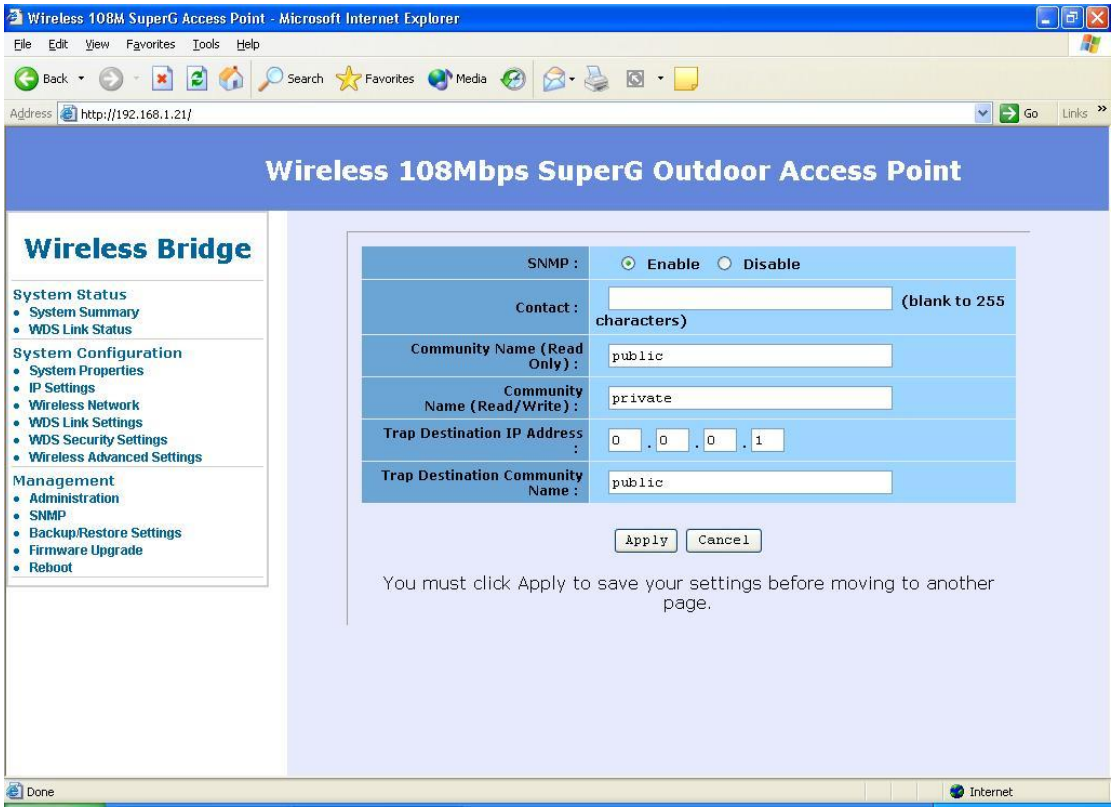
- **No Security –** Both Point to Point and Point to Multi-Point traffic transmit without encryption
- **WEP –** Both Point to Point and Point to Multi-Point traffic are encrypted by the same WEP key
- **WPA-PSK** – The Point to Point and Point to Multi-Point work in WPA-PSK **(TKIP)** mode and WPA-PSK **(AES)** mode

Changing SNMP Settings

Under System Configuration, click **SNMP** to display and change settings for the Simple Network Management Protocol.

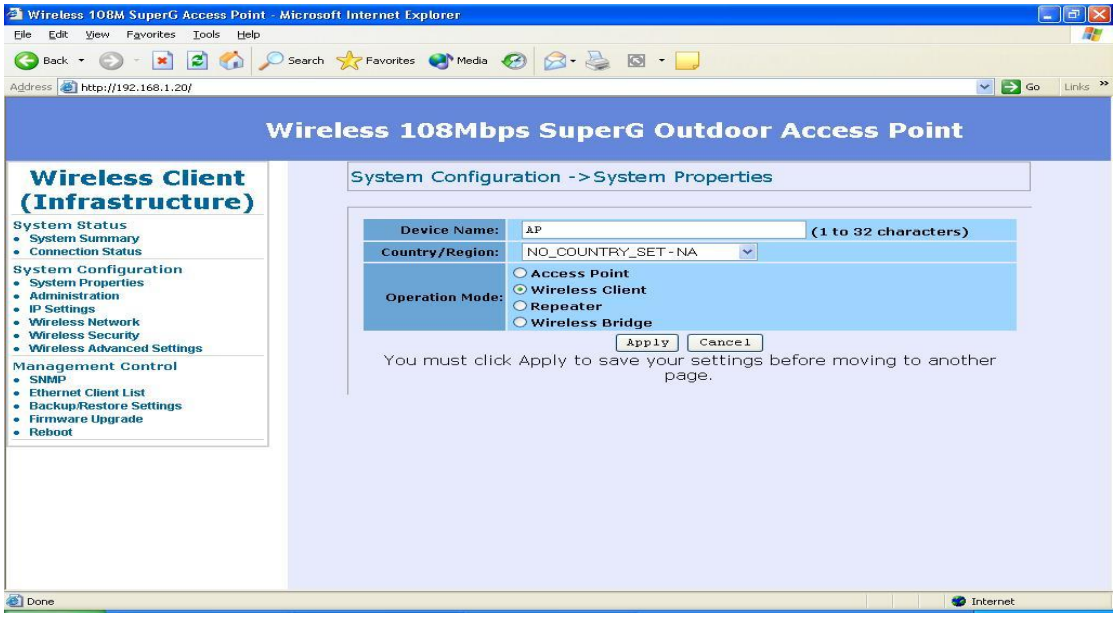
To communicate with the access point, the **SNMP** agent must first be enabled and the Network Management Station must submit a valid community string for authentication. Select **SNMP** Enable and enter data into the fields as described below. When you are finished, click **“Apply”**

Setting	Description
SNMP	Enables or disables SNMP.
Contact	Sets the location string that describes the system location. Maximum length is 255 characters.
Community Name (Read Only)	Specifies a community string with read-only access. Authorized management stations are able to retrieve MIB objects. Maximum length is 32 characters.
Community Name (Read Write)	Specifies a community string with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. Maximum length is 32 characters.
Trap Destination IP Address	Enter the IP address of the trap manager that will receive these messages.
Trap Destination Community Name	Enter the community name of the trap manager that will receive these messages.


Wireless 108M SuperG Access Point - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.21/
Go Links
Wireless 108Mbps SuperG Outdoor Access Point
Wireless Bridge
System Status
System Summary
WDS Link Status
System Configuration
System Properties
IP Settings
Wireless Network
WDS Link Settings
WDS Security Settings
Wireless Advanced Settings
Management
Administration
SNMP
Backup/Restore Settings
Firmware Upgrade
Reboot
SNMP : Enable Disable
Contact : (blank to 255 characters)
Community Name (Read Only) : public
Community Name (Read/Write) : private
Trap Destination IP Address : 0 . 0 . 0 . 1
Trap Destination Community Name : public
Apply Cancel
You must click Apply to save your settings before moving to another page.
Done
Internet

Wireless Configuration – Wireless Client Mode

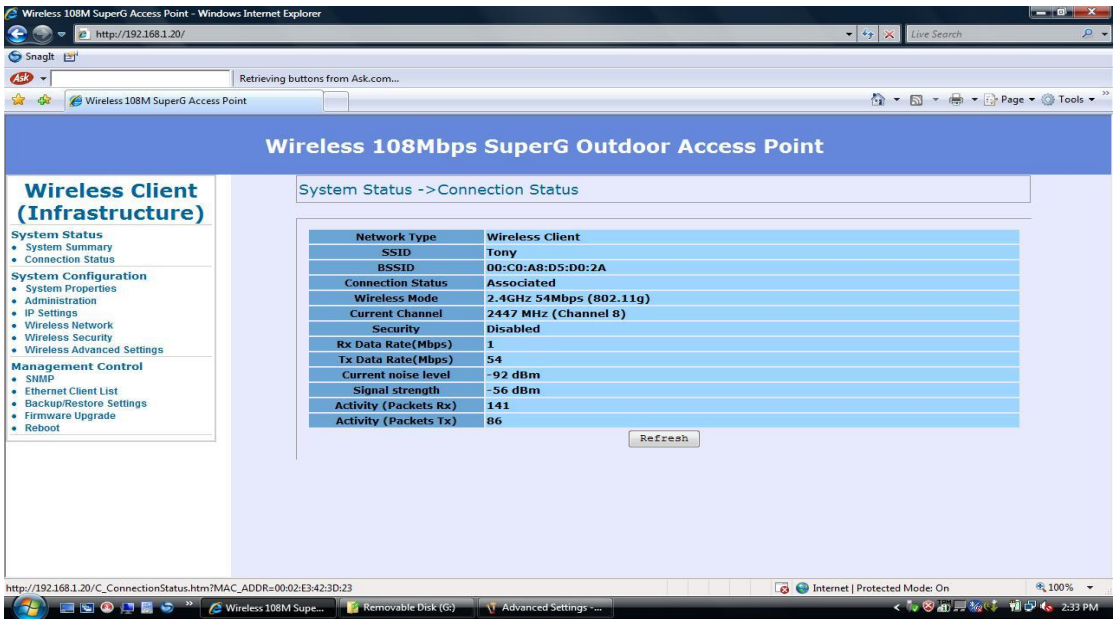
AP can also work as an Ethernet client bridge to connect up to 16 Ethernet device into wireless network. In order to setup the AP to work in Ethernet bridge mode, you need to choose "**Wireless Client**" mode and click "**Apply**" at System Properties page. After need to reboot the AP to make sure the AP work in client mode.



After the system reboot is done, you can see the page as below. Status page show the AP is now working in Wireless Client mode.

Connection Status -

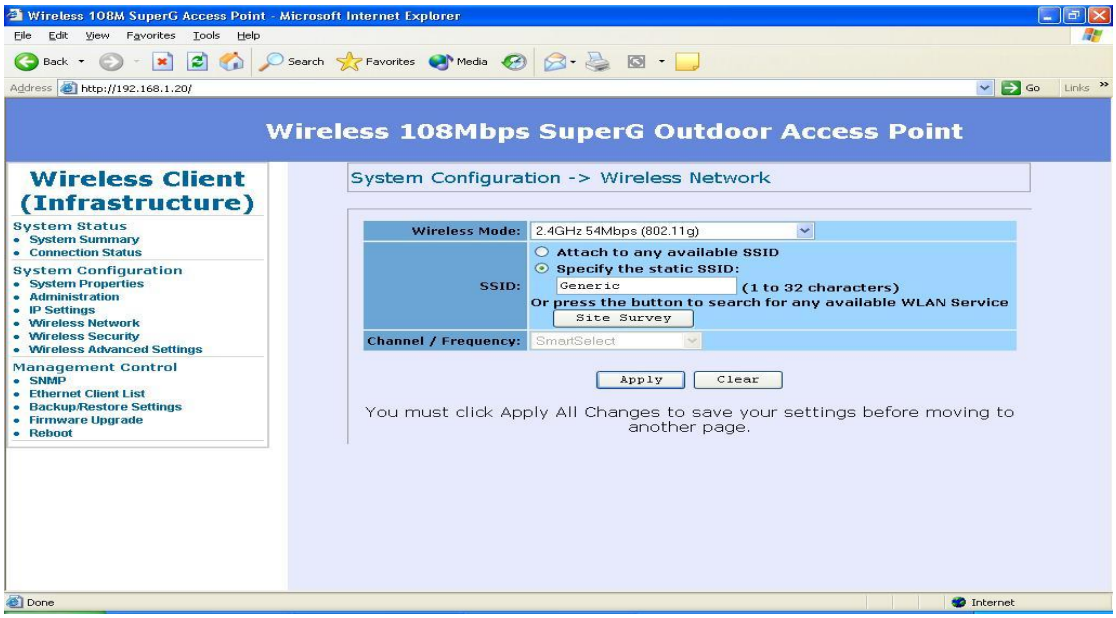
- **Connection –** This column show current connection status. If AP already connect to an Access Point or station, here will show the MAC address of the associated Access Point or station. Otherwise, connection column will show **"N/A"** which means no connection to any Access Point or station.
- **Network Type –** Here indicates the Access Point works in AP mode or Client mode (Infrastructure mode / Ad Hoc mode)
- **SSID –** SSID column displays current SSID assigned to the AP
- **BSSID –** BSSID
- **Wireless Mode –** Here show the Access Point current work in either 11b or 11g mode
- **Current Channel –** This column indicates the radio channel currently in use.
- **Security –** Here indicates AP security settings in client mode. Should be either **"Disabled"**, **"WEP"** or **'WPA-PSK"**.
- **Rx Data Rate(Mbps) –**show the current Rx Data rate status
- **Tx Data Rate(Mbps) –**show the current Tx Data rate status
- **Current noise level –**This column shows current link quality with AP by noise level in 0 to -96 dBm scale.
- **Signal strength –** This column shows current link quality with AP by signal strength in 0 to -96 dBm scale.
- **Activity (Packets Rx) –**show the current Rx packets
- **Activity (Packets Tx) –**show the current Rx packets



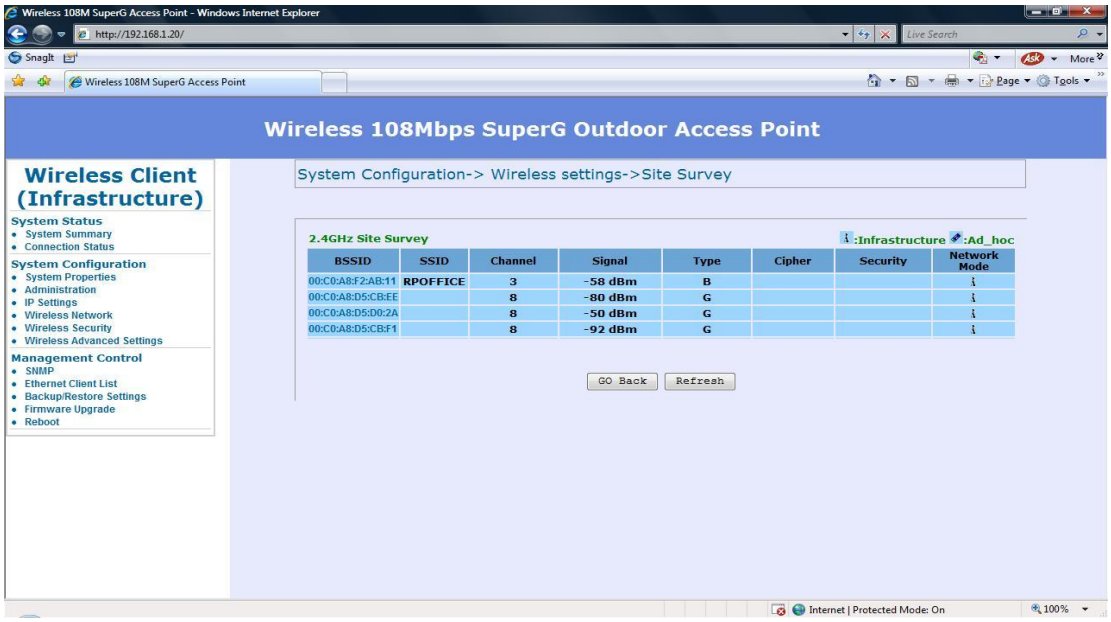
Wireless Network -

- **Network Mode –** You can set the wireless client into 2 different modes by clicking radio button. Wireless Client (Infrastructure) act as an AP client while Ad-hoc can support peer to peer network. Both Infrastructure and Ad-hoc can support up to 108M SuperG transmission.
- **Wireless Mode -** Default setting is **"2.4GHz 54Mbps (802.11g)"**. This will support all 802.11b/g clients connect to the AP. You can choose **"2.4GHz 11Mbps (802.11b)"** in wireless mode column if your environment only have 802.11b clients. The final selection **"2.4GHz 108Mbps (802.11 SuperG)"** supports high speed 108Mbps SuperG function. In order to support SuperG 108M transmission, all wireless clients will need to be Atheros® solution.
- **SSID -** The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. You can choose "**Attach to any available SSID"**; system will determine the Access Point currently available and establish connection with that Access Point. If you already understand your wireless environment well, you can type in the SSID in **"Specify the static SSID"** manually.

At Wireless Network page you can find a "**Site Survey**" button as shown below. You can easily click on the "**Site Survey**" to find all wireless networks available in your current environment.



The Site Survey page can help you identify all the APs currently working in your environment. Just easily click on the BSSID column, the system will join you to the SSID you specify. In the Site Survey page you can also see the details of all SSID currently available.



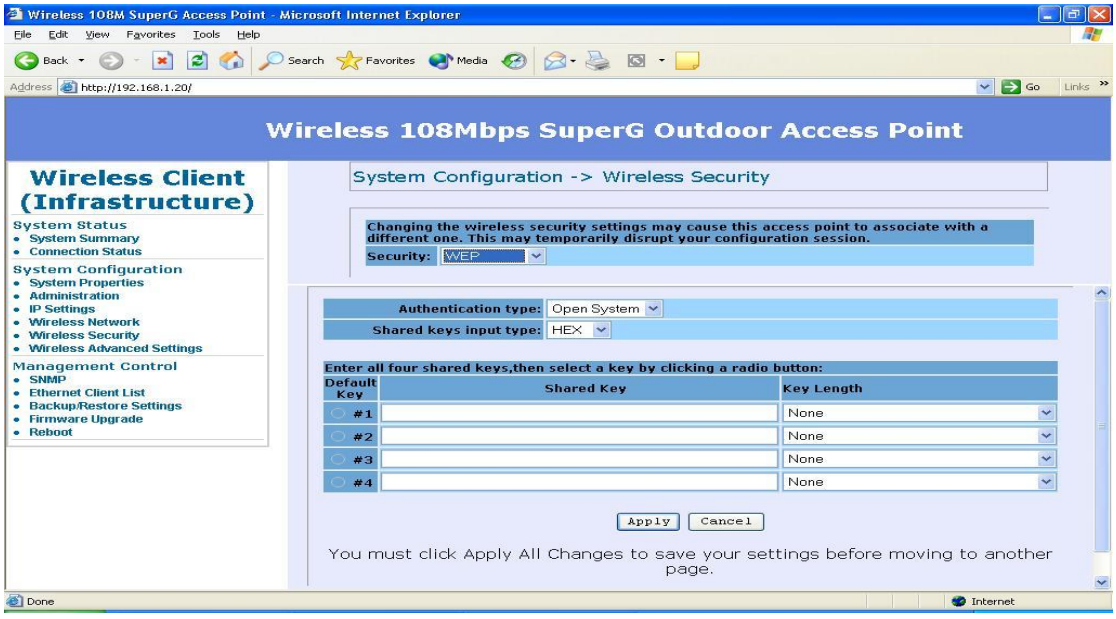
After you determine which AP (SSID) to join, you can click on the BSSID column your want to choose. The system will automatically join the SSID you specified after reboot.

Wireless Security –

WEP is a basic encryption method, which is not as secure as WPA. To use WEP as a client, you will need to input a transmit key and a level of WEP encryption exactly the same as the Access Point.

- **Shared keys input type –** Select HEX or ASCII depends on your preference
- **Key table –** You can input 4 different WEP encryption keys into the table and by choosing the radio button to decide which one is valid now. The AP supports 64, 128 and 152bit key length. The longer key we choose usually means the encryption is stronger.

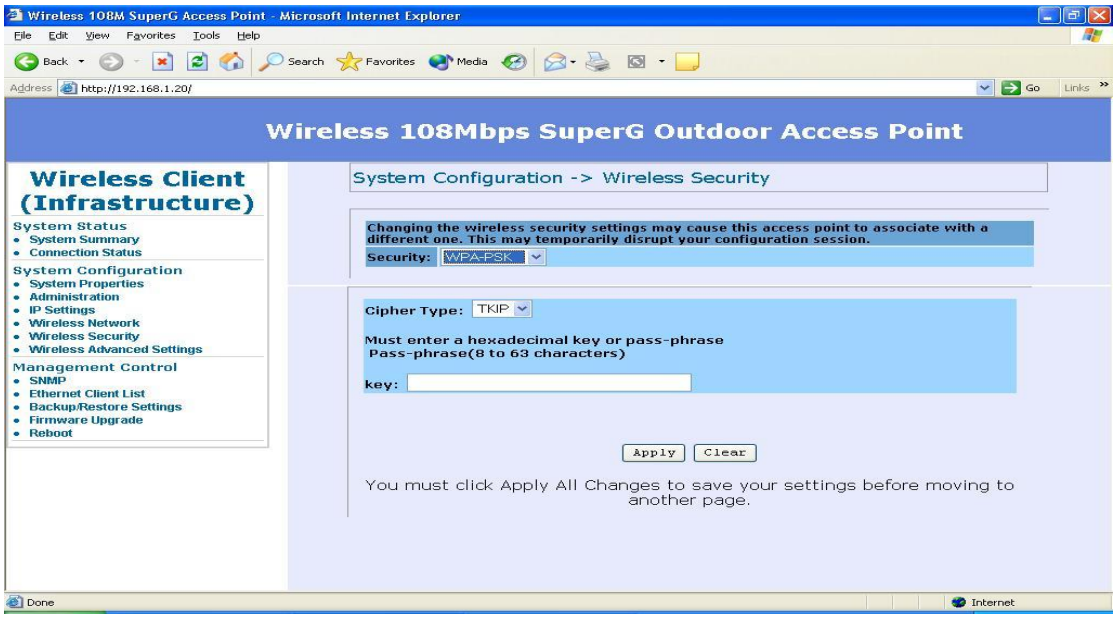
After all changes are made, be sure to click on **"Apply"** to make sure all changes are saved into system.



WPA-PSK stands for Wi-Fi Protected Access – Pre-Shared Key. WPA-PSK is design for home users who do not have RADIUS server in their network environment. WPA can provide better security level than WEP without difficult setting procedure.

- **PassPhrase Key -** Enter a WPA Shared Key of 8-63 characters. The Shared Key should be also applying the Access Point work in the same wireless network.
- **Cipher Type -** WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**.

Remember to click on **“Apply”** to make sure all changes are made before leaving this page.



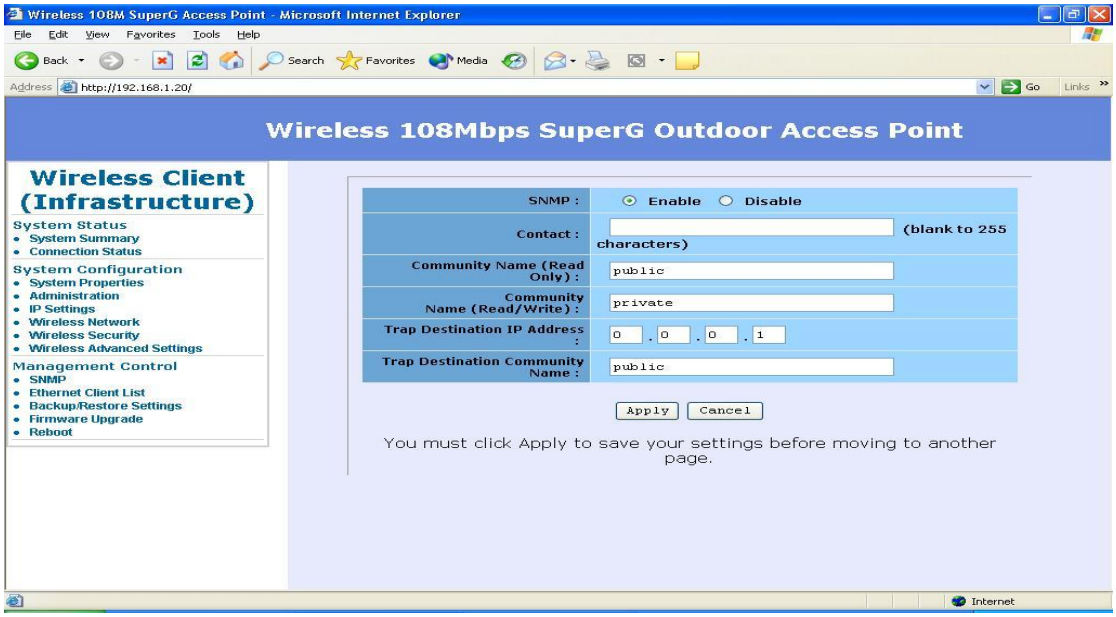
Changing SNMP Settings

Under System Configuration, click **SNMP** to display and change settings for the Simple Network Management Protocol.

To communicate with the access point, the **SNMP** agent must first be enabled and the Network Management Station must submit a valid community string for authentication. Select **SNMP** Enable and enter data into the fields as described below. When you are finished, click **“Apply”**

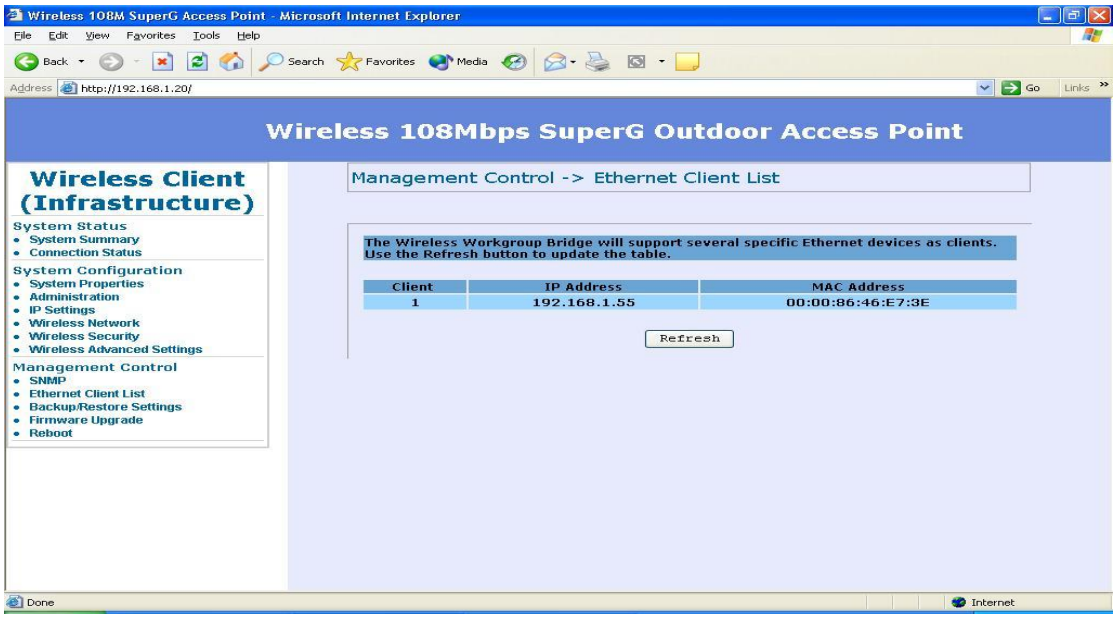
Setting	Description
SNMP	Enables or disables SNMP.
Contact	Sets the location string that describes the system location. Maximum length is 255 characters.
Community Name (Read Only)	Specifies a community string with read-only access. Authorized management stations are able to retrieve MIB objects. Maximum length is 32 characters.
Community Name (Read Write)	Specifies a community string with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. Maximum length is 32 characters.
Trap	Enter the IP address of the trap manager that will receive

Destination IP Address	these messages.
Trap Destination Community Name	Enter the community name of the trap manager that will receive these messages.



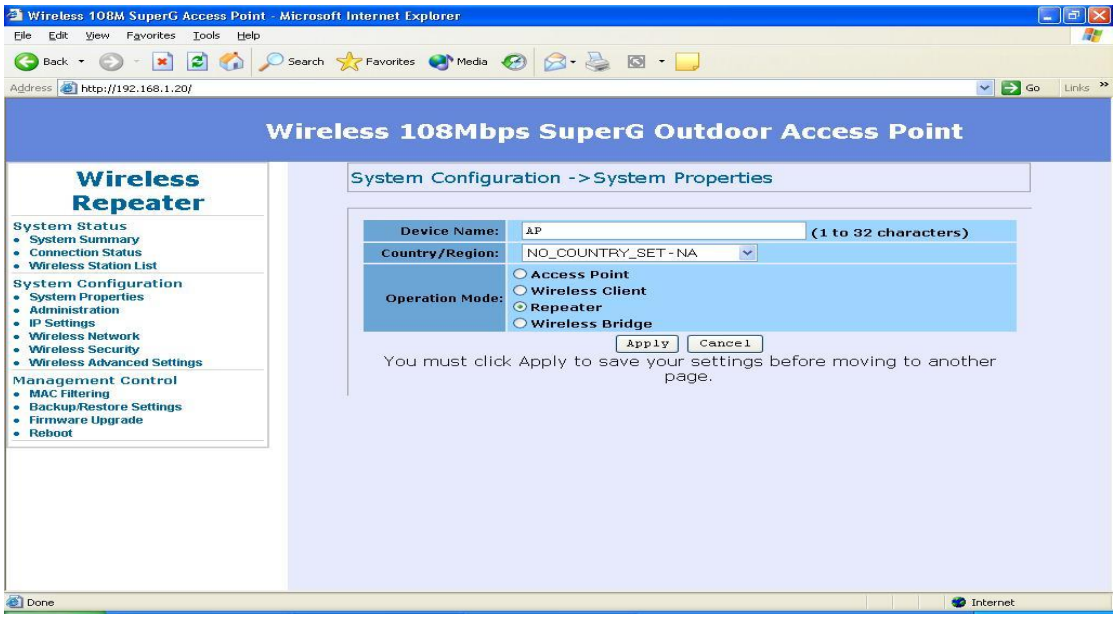
Ethernet Client List –

In Ethernet Client List page, you can check all the details here including IP Address and MAC Address. Press **"Refresh"** if you add any new Ethernet client into network. The page will update latest status of current Ethernet network.



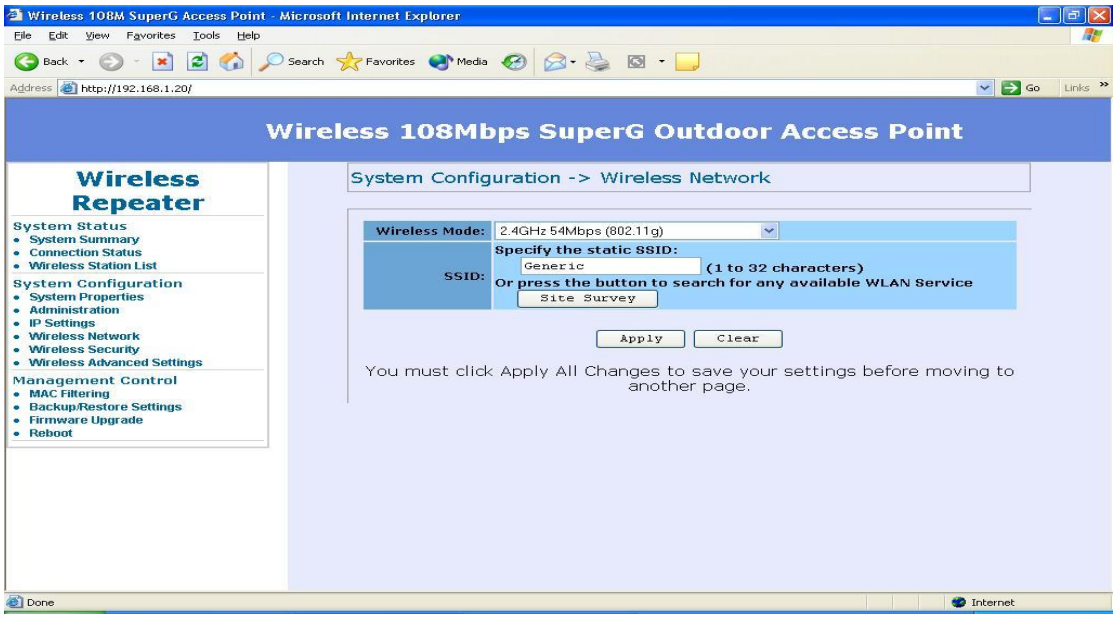
Wireless Configuration – Wireless Repeater Mode

When set the Access Point to Repeater mode, the AP is able to talk with one remote access point within its range and retransmit its signal. In order to setup the AP to work in Ethernet bridge mode, you need to choose "**Repeater**" mode and click "**Apply**" at System Properties page. After need to reboot the AP to make sure the AP work in repeater mode.

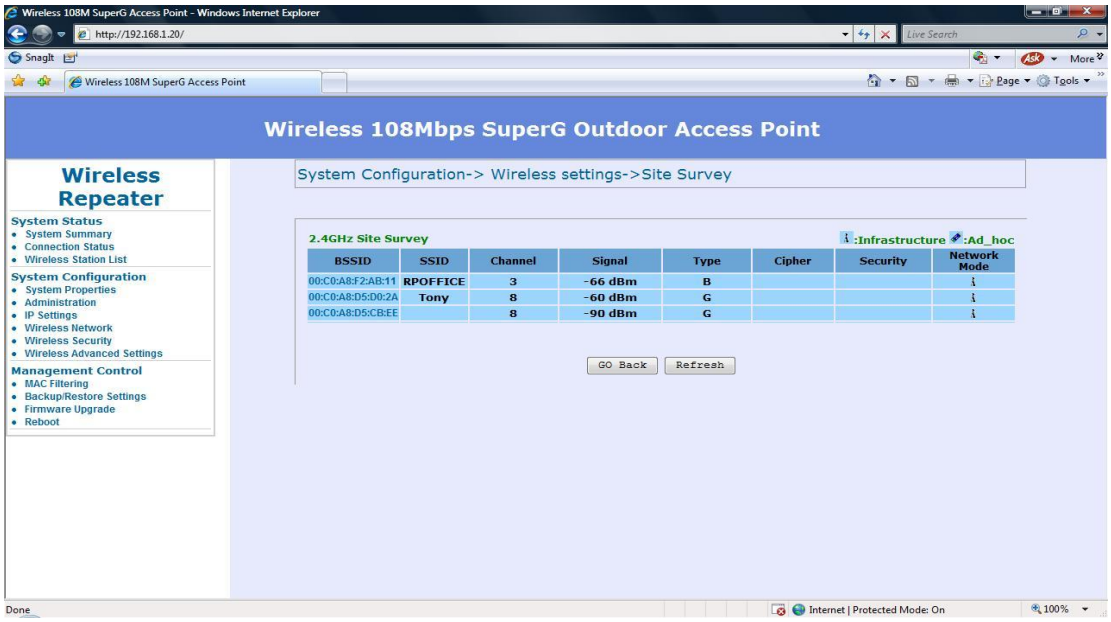


After enable the repeater mode, you can click on "**Wireless Network**" and choose "**Site Survey**" to pick one of the SSIDs you would like to retransmit its signal. (Please be awarded that while using the repeater mode, the throughput performance maybe nearly only half compare with access point mode.

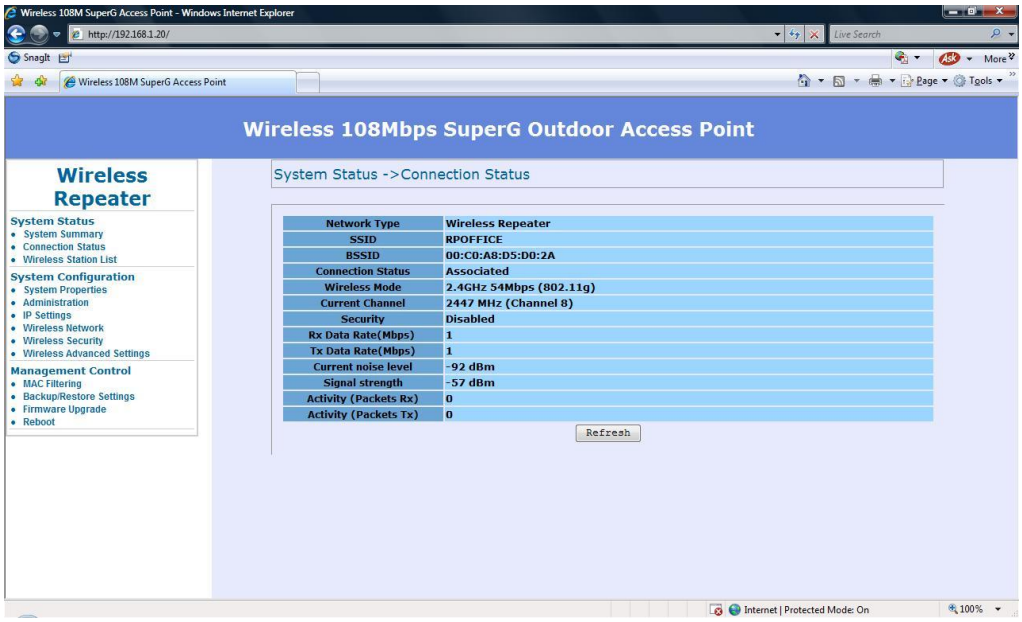
Because the repeater needs to communicate with original AP and also the clients associate to the repeater at the same time.)



After click on the "**Site Survey**" button, you can choose the Access Point you need to extend its range by clicking on "**BSSID**" column. Then "**Apply**" the change to make sure system working properly with new setting.



After all the changes are made, you can check the "**Connect Status**" page to check current SSID and link quality / signal strength. Some more information are all available at this page.


Wireless 108M SuperG Access Point - Windows Internet Explorer
http://192.168.1.20/
Wireless 108M SuperG Access Point
Wireless 108Mbps SuperG Outdoor Access Point
Wireless Repeater
System Status
System Summary
Connection Status
Wireless Station List
System Configuration
System Properties
Administration
IP Settings
Wireless Network
Wireless Security
Wireless Advanced Settings
Management Control
MAC Filtering
Backup/Restore Settings
Firmware Upgrade
Reboot
System Status ->Connection Status
Network Type | Wireless Repeater
SSID | RPOFFICE
BSSID | 00:C0:A8:D5:D0:2A
Connection Status | Associated
Wireless Mode | 2.4GHz 54Mbps (802.11g)
Current Channel | 2447 MHz (Channel 8)
Security | Disabled
Rx Data Rate(Mbps) | 1
Tx Data Rate(Mbps) | 1
Current noise level | -92 dBm
Signal strength | -57 dBm
Activity (Packets Rx) | 0
Activity (Packets Tx) | 0
Refresh
Internet | Protected Mode: On
100%

Appendix A: Glossary

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and anoperating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

Download - To receive a file transmitted over a network.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Gateway - A device that interconnects networks with different, incompatible communications

protocols.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Node - A network junction or connection point, typically a computer or work station.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

Upgrade - To replace existing software or firmware with a newer version.

WEP (**W**ired **E**quivalent **P**rivacy) - An optional cryptographic confidentiality algorithm specified by IEEE 802.11 that may be used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy confidentiality.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix B: Specification

Standard support	IEEE802.11b IEEE802.11g IEEE802.3 IEEE802.3u
Interface	Wireless IEEE802.11b/g One 10/100 RJ-45 port
SDRAM	8Mbyte
Flash	2Mbyte
Max. Bandwidth Ethernet Wireless	 Full Duplex: 200Mbps (for 100BASETX), 20Mbps (for 10BaseT) Half Duplex: 100Mbps (for 100BaseTX), 10Mbps (for 10BaseT) 1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54, 108Mbps Auto Fall-Back
Wireless Radio	Data Rate 1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54 and 108Mbps Signal Frequency 2.4Ghz to 2.5Ghz OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK Encryption 64bit / 128bit and 152bit WEP data encryption Channel America/FCC：2.412~2.462 GHz (11 channels) Europe CE/ETSI：2.412~2.472 GHz (13 channels) RF Power Output: 20dBm at 11Mbps / 20dBm at 54Mbps (typical) Receiver Sensitivity: 54Mbps OFDM, 10% PER, -64dBm 11Mbps CCK, 8% PER, -86dBm
Wireless Setting	– Operation Mode – AP / Wireless Client / Repeater / Wireless Bridge Point to Point and Point to Multi-Point Mode – SSID – Channel Selection – Transmission Rate (Best, 108, 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1) in Mbps – Transmit power (Full, Half, Quarter, Eighth, Minimum) – Beacon Interval (20-1000): 100 – Data Beacon Rate (DTIM (1-16384): 1 – Fragment Length (256-2346): 2346

	– RTS Threshold (256-2346): 2346 – Short Preamble: Enable – Allow 2.4GHz 54Mbps Station Only – Protection Mode: Auto / Enable / Disable – Distance
Wireless Security	WEP setting – Authentication type: Open System / Shared Key – Shared keys input type: HEX / ASCII – Shared keys length: (64-bit, 128-bit, 152-bit) – Default WEP Key to use (1-4) WPA-PSK setting – PassPhrase – WPA Cipher Type (Auto, TKIP, AES) – Group Key Update Interval: 300 WPA setting – Radius Server IP Address – Radius Port: 1812 – WPA Cipher Type (Auto, TKIP, AES) – Shared Key – Group Key Update Interval: 300
Software / Firmware	– Site Survey – DHCP Client – Suppressed SSID – Station separation – Wireless access control by MAC address (deny or accept) – WPA Support (WPA personal and enterprise) – Web-based configuration via popular browser (MS IE, Netscape…) – Windows “Locator” program to help find IP in DHCP client mode – Firmware upgrade and configuration backup via Web – Reset to default by WebUI – SNMP v1/v2
Forwarding Mode	Store and Forward

Appendix C: Specification

Please refer to the following system grounding diagram for your installation reference.
When in doubt, refer to the NEC code to determine proper grounding techniques.
For detailed information regarding grounding the outdoor wireless system.